2/2021

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

44. Jahrgang
ISSN 0137-7767
14,00 Euro



Bildung

■ Datenschutz als Bildungshindernis in Corona-Zeiten? ■ Die Grundrechte dürfen nicht unter die Räder kommen! ■ Datenschutzfreundlicher Unterricht ■ Wie ein Lock-In an Schulen der Gesellschaft schadet ■ „Datenschutz geht zur Schule" (DSgzS) ■ Bildungsmedien für Schulen – bundesweites Kuddelmuddel ■ Sündenbock Datenschutz ■ Polizeirechtsreform in Schleswig-Holstein ■ Pressemitteilungen ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Samstag, 1. August 2021,
Redaktionsschluss DANA 3/2020
Schwerpunkt: eGovernment

Samstag, 4. September 2021,
DVD-Mitgliederversammlung
(Bonn)

Dienstag, 21. September 2021,
Computas Datenschutztag 2021
(Köln und virtuell)

Dienstag, 28. September 2021,
Tag der Informationsfreiheit 2021

Mittwoch und Donnerstag,
27.10./28.10.2021 & Behördentag
am Freitag, dem 29.10.2021,
BvD-Herbstkonferenz,
Nürnberg (Hybrid-Veranstaltung)

Samstag, 01. November 2021,
Redaktionsschluss DANA 4/2021,
Schwerpunkt: ePrivacy-Verordnung,
Veränderung des Datenschutzrechts

Foto: Pixabay..com

DANA
Datenschutz Nachrichten
ISSN 0137-7767
44. Jahrgang, Heft 2

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftsstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Markus Eßfeld, Riko Pieper, Frank Spaeing
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autorinnen und Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 14 Euro. Jahresabonnement 48 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, Pixabay, shutterstock, iStock, BvD

Editorial


Bild: iStock.com/ Imgorthand

Datenschutz in Schulen und Bildungseinrichtungen ist ein weites und interessantes Themenfeld, das schon länger auf dem Wunschzettel der DANA-Redaktion stand. Bereits im Jahr 2011 gab es ein Heft mit dem Titel „Datenschutz in Schulen". Seinerzeit forderte Hajo Köppen im Leitartikel „Datenschutzpraxis an Schulen – Nachsitzen ist angesagt!" und die Landesdatenschutzbeauftragten setzten sich für die Entwicklung und Stärkung der Medienkompetenz von Schülern und Lehrern ein.

Zehn Jahre später sind beide Anliegen (leider) immer noch hochaktuell. In einem Einführungsartikel zum Schwerpunkt werden die verschiedenen Artikel vorgestellt.

Außerdem haben wir in dieser Ausgabe noch einen Artikel von Ulrich Kelber zum Datenschutzbashing, einen Artikel von Thilo Weichert zur Polizeirechtsreform in Schleswig-Holstein, sowie Pressemitteilungen und offene Briefe befreundeter Organisationen.

Abschließend versprechen die Datenschutznachrichten aus dem In- und Ausland sowie die Rechtsprechungsübersicht und die Buchbesprechungen weitere Anregungen.

Wir wünschen Ihnen eine schöne Sommerzeit!
Markus Eßfeld, Riko Pieper und Frank Spaeing

Autorinnen und Autoren dieser Ausgabe:

Markus Eßfeld, Vorstandsmitglied in der DVD, essfeld@datenschutzverein.de

Prof. Dieter Kugelmann, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, https://datenschutz.rlp.de

Dr. Lutz Hasse, Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit, https://www.tlfdi.de

Jessica Wawrzyniak, Medienpädagogin bei Digitalcourage e.V., www.digitalcourage.de, www.kidsdigitalgenial.de

Thomas Freihorst, ehrenamtliches Mitglied des Bildungsprojekts „Chaos macht Schule" des CCC, hauptberuflich Lehrer in Hannover, https://ccc.de/schule

Steffen Haschler, ehrenamtliches Mitglied des Bildungsprojekts „Chaos macht Schule" des CCC, hauptberuflich Lehrer in Heidelberg, https://ccc.de/schule

Benjamin Schlüter, Informatiker und ehrenamtliches Mitglied des Bildungsprojekts „Chaos macht Schule" des CCC, https://ccc.de/schule

Riko Pieper, Vorstandsmitglied in der DVD, pieper@datenschutzverein.de

Frank Spaeing, Vorstandsmitglied in der DVD, spaeing@datenschutzverein.de

Dr. Joachim Paul, wissenschaftlicher Referent im öffentlichen Dienst, jpaul@xpertnet.de

Prof. Ulrich Kelber, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, www.bfdi.de

Dr. Thilo Weichert, Vorstandsmitglied in der DVD, weichert@datenschutzverein.de

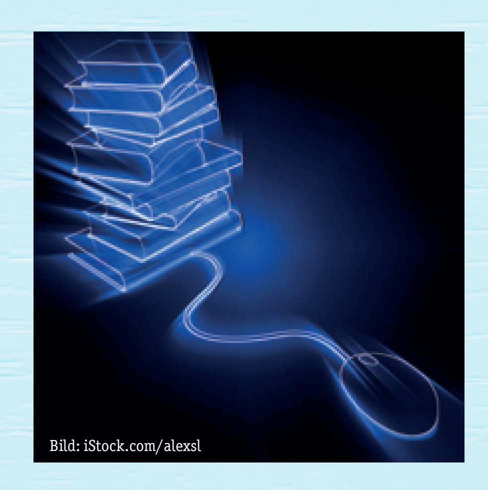
Markus Eßfeld

Datenschutz in Schulen und Bildungseinrichtungen

Datenschutz hat seine unionsrechtliche Grundlage in Artikel 8 der Charta der Grundrechte der Europäischen Union und sein verfassungsrechtliches Fundament im informationellen Selbstbestimmungsrecht. Er genießt grundrechtlichen Schutz. Sind die Betroffenen Kinder und Jugendliche beim Schulbesuch, rücken weitere Rechtsvorschriften in den Fokus. Zu nennen wäre Artikel 7 Grundgesetz, wonach das Schulwesen unter der Aufsicht des Staates steht. Zu denken wäre an Artikel 6 Grundgesetz, der das Wächteramt des Staates bei der Erziehung der Kinder festschreibt. Zahlreiche Gesetzesvorschriften ohne Verfassungsrang wären aufzuzählen. Zustimmung dürfte der Grundsatz finden, dass Kinder und Jugendliche besonders schützenswert sind und dass dieses Postulat zu berücksichtigen ist, wenn es um ihren Umgang mit dem Internet und damit verbundener elektronischer Kommunikationstechnik geht. Aber dabei bleibt es nicht: Auch Lehrer und Eltern zählen zu den schützenswerten Akteuren im schulischen Bereich. Die Aufrechterhaltung der Schulpflicht in Pandemiezeiten war dabei eine besondere Herausforderung, die Schüler, Eltern und Lehrer auf jeweils andere Weise, aber mit gleicher Stärke getroffen hat! Während es im ersten Quartal 2020 zunächst um technische Unzulänglichkeiten bei der Umstellung auf den digitalen Fernunterricht ging, haben im Pandemieverlauf weitere Fragen an Brisanz gewonnen. Dazu gehört im Allgemeinen die Fähigkeit der beteiligten Akteure, mit der Informationstechnik des Internets umzugehen sowie der datenschutzkonforme Umgang mit den dabei preisgegebenen Daten. Die Klagen über fehlende Medienkompetenz und mangelnde Sensibilisierung für den Datenschutz im schulischen Bereich sind alt: Bereits in der DANA 4/2011, mithin vor fast 10 Jahren (!), findet sich ein entsprechender Aufruf des niedersächsischen Landesdatenschutzbeauftragten zur Entwicklung der Medienkompetenzen der Schüler. Seither waren die technische Entwicklung und die damit verbundenen Herausforderungen enorm; die Nutzung des Internets hat auch an Schulen erheblich zugenommen. Ob das Wissen um den Datenschutz und die Fähigkeiten beim Umgang mit den nicht mehr ganz so neuen Medien damit Schritt gehalten haben, ist höchst fragwürdig. Verdienstvoll ist hier die in dieser DANA-Ausgabe beschriebene Initiative des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V. namens „Datenschutz geht zur Schule“ (DSgzS) (ab Seite 85).

Zahlreiche beruflich mit dem Datenschutz befasste Personen sind seit vielen Jahren ehrenamtlich in den Schulen aktiv und versuchen, bei Schülern und Lehrern mehr Kompetenzen im Umgang mit elektronischen Medien zu schaffen und das Bewusstsein für das Recht auf informationelle Selbstbestimmung zu fördern. Der Erfolg ist beachtlich!

Die Probleme allerdings auch. Zu Recht beklagt der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit, Dr. Lutz Hasse, die großen Defizite im Medienkundeunterricht (ab Seite 73). Insbesondere den Hochschulen fehle es an Strategie und Systematik. Die Lehrpläne müssten in diesem Bereich regelmäßig angepasst werden. Der Kenntnisstand von Lehrern und Schülern zu informationstechnologischen Fragen sei nicht ausreichend entwickelt. Diese Erkenntnis ist leider nicht neu. Erfreulich ist, dass sie – pandemiebezogen – in jüngerer Zeit mehr Beachtung erfährt: So hat beispielswei-


Bild: iStock.com/alexsl

se das Brandenburgische Ministerium für Bildung, Jugend und Sport ein umfangreiches und instruktives Papier für die weitere Diskussion formuliert[1] und die Brandenburger Landesregierung dem Landtag einen Gesetzentwurf vorgelegt, der die Nutzung digitaler Lehr- und Lernmittel legitimieren soll[2].

Mit einer Legitimierung digitaler Lehrmittel im Schulgesetz ist es freilich nicht getan. Die Hausaufgabenliste für die gestaltenden Akteure, nicht zuletzt für die obersten Kultusbehörden der Bundesländer, ist lang. Da wird man über den drohenden Lock-In-Effekt an Schulen nachdenken und darauf reagieren müssen (beachten Sie dazu den Artikel ab Seite 79). Mit diesem Begriff aus der Betriebswirtschaftslehre ist die Abhängigkeit gemeint, in die u.a. Schulen sich begeben, wenn sie sich beim Kauf überstürzt in eine besondere Bindung an einen bestimmten Hersteller von Hardware- und Software-Produkten begeben und damit konzeptlos eine langfristige Abhängigkeit begründen, die der Schule und den Schülern nur schaden kann. Mangels Fachpersonal vor Ort ist es nicht einfach, hier den richtigen Weg zu finden. Einen lesenswerten Aufsatz dazu verfasste Jessica Wawrzyniak, der sich mit Problemen datenschutzfreundlichen Unterrichts beschäftigt (ab S. 76).

Nachgedacht wird auch über die Rechtmäßigkeit der Nutzung von Microsoft Office 365. Die Bedenken sind erheblich; beispielsweise der Baden-Württembergische Landesbeauftragte für Datenschutz und Informationsfreiheit rät von der Nutzung ab[3] (siehe auch die dazugehörige Presseerklärung auf S. 102). Begrüßenswert sind die Verhandlungen zwischen dem amerikanischen Konzern und der Datenschutzkonferenz[4], dessen Ergebnis in Fachkreisen mit Spannung erwartet wird.

Während der in dieser Ausgabe für einen Artikel interviewte Thüringische Landesbeauftragte für Datenschutz und Informationsfreiheit auf den großen Kenntnisunterschied zwischen chinesischen und deutschen Schülern hinweist, was die Algorithmenkenntnisse angeht, eignet sich ein anderes Land eher für eine Vorbildrolle: So enthält der neue Entwurf des nationalen australischen Lehrplanes einen besonderen Schwerpunkt zur Ausbildung der Schüler in „Cybersecurity“[5]. Die Unterrichtsreihe beginnt schon bei den Fünfjährigen und enthält genauere Vorgaben für die einzelnen Altersgruppen bis hin zur „late primary school“ für elfjährige Schüler. Es fängt bei den Kleinsten an mit einer Sensibilisierung der Verwendung einfacher personenbezogenen Daten und geht bis zum Lernen des respektvollen Umgangs mit anderen Meinungen für die Elfjährigen.

Neben dem Artikel zum Lock-In-Effekt haben wir uns bei dieser Ausgabe noch eines zweiten Artikels aus der sehr lesenswerten heise.de-Artikelserie[6] mit freundlicher Genehmigung des Heise-Verlags wie auch der Autoren bedienen dürfen: Joachim Paul kommentiert das bundesweite Kuddelmuddel bei digitalen Bildungsmedien für Schulen (ab Seite 94).

Der Datenschutz ist schuld![7] Dieser Satz ist nicht neu. Er bleibt ärgerlich. Man hört ihn meist aus unberufenem Mund. Im Jahr 2 der Pandemie hört man ihn, wohl populistisch motiviert, wieder öfter. Zweifellos werden auch im schulischen Bereich Daten, auch besonders sensible Daten nach Art. 9 DSGVO, erhoben. Dass das aber einer Kontrolle und eines Konzeptes bedarf, müsste sich von selbst verstehen. Wie wichtig der grundrechtsbezogene Datenschutz ist, muss immer wieder neu erklärt werden. Dass Datenschutz kein Bildungshindernis in Pandemiezeiten ist, stellt Prof. Kugelmann, der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, in einem Artikel (ab Seite 70) fest.

Denn „den Datenschutz aus Gründen medialer Effekthascherei kaputt zu reden, ist brandgefährlich“.

Einen Artikel des Bundesbeauftragten[8] dazu finden Sie in diesem Heft (ab S. 99). Auch die Berliner Beauftragte für den Datenschutz und die Informationsfreiheit hat sich zusammen mit ihrem Kollegen aus Rheinland-Pfalz zu diesem Thema geäußert[9].

Für den Schwerpunkt dieses Heftes sei abschließend ein Satz der Berliner Beauftragten zitiert:

„Wenn gefordert wird, dass die Digitalisierung der Schulen datenschutzgerecht erfolgen muss, dient das nicht der Verhinderung einer Digitalisierung der Schulen, sondern vielmehr einer nachhaltigen Entwicklung“.

So ist es!

1 Diskussionsgrundlage: Perspektiven des Lernens mit digitalen Medien an Schulen in Brandenburg, https://mbjs.brandenburg.de/media_fast/6288/19-21_anhang_diskussionsgrundlage_digitalisierungsstrategie_schulen_bb.pdf

2 https://www.parlamentsdokumentation.brandenburg.de/starweb/LBB/ELVIS/parladoku/w7/drs/ab_3500/3504.pdf

3 Die Bedenken des Landesbeauftragten für Datenschutz, Stefan Brink, gegen die vom Kultusministerium geplante Nutzung der Software Microsoft Office 365 sind gravierender als bisher bekannt, https://www.badische-zeitung.de/gravierende-bedenken-wegen-datenschutzes--201498263.html

4 Im Interview mit Dr. Lutz Hasse, auf Seite 73 dieser DANA

5 Schneier on Security, https://www.schneier.com/blog/archives/2021/05/teaching-cybersecurity-to-children.html, posted on May 7th, 2021

6 https://www.heise.de/hintergrund/Schule-digital-Wie-ist-der-Status-Quo-Was-hat-sich-veraendert-5993043.html

7 Wie es der Zufall so will, wurde einer der bekannteren Vertreter dieser ärgerlichen These am 11.06.2021 mit einem BigBrotherAward 2021 verdientermaßen geehrt: https://bigbrotherawards.de/2021/public-intellectual-julian-nida-ruemelin

8 für den Datenschutz und die Informationsfreiheit

9 https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/2021-BlnBDI-LfdRLP-Standpunkt_Attacke_auf_Datenschutz.pdf

Prof. Dieter Kugelmann

Datenschutz als Bildungshindernis in Corona-Zeiten?

Seit über einem Jahr prägt die Corona-Pandemie unser aller Leben. Neben tiefgreifenden Einschränkungen ist auch zu verzeichnen, dass die Digitalisierung verstärkt Fahrt aufgenommen hat. So hat das Homeschooling dazu geführt, dass digitale Lern- und Lehrmittel verstärkt genutzt werden mussten. Folgerichtig sind vielfältige Fragen des Datenschutzes in den Fokus gerückt worden. Immer mehr personenbezogene Daten werden gesammelt, sei es bei der Kontaktnachverfolgung oder beim Nachweis der Befreiung von der Maskenpflicht; das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger steht zunehmend unter Druck. Dies betrifft insbesondere auch den Bildungsbereich und vor allem jüngere Menschen – Kinder und Jugendliche, die nunmehr auch im Unterricht viel Zeit mit digitalen Anwendungen verbringen, aber oft auch von sich aus neue Angebote ausprobieren. Dabei ist zu beachten, dass es mit Blick auf Kinder bereits in der Datenschutz-Grundverordnung im Erwägungsgrund 38 heißt: „Kinder verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind."

Nicht nur in Corona-Zeiten, aber angetrieben durch die Pandemie gilt es daher, ein besonderes Augenmerk auf den Datenschutz von Minderjährigen zu legen und hierbei insbesondere die Möglichkeiten im Bildungsbereich zu erörtern. Anhand von drei Themenbereichen, die während der Pandemie große Aufmerksamkeit erfahren, soll dies hier geschehen:

Schulunterricht von Zuhause

Eine der zentralen Fragen ist, unter welchen Bedingungen und mit welchen digitalen Anwendungen ein datenschutzkonformer Schulunterricht von Zuhause möglich ist. Grundsätzlich gilt, dass sichergestellt sein muss, dass die Vertraulichkeit der Unterrichtssituation gegenüber Dritten gewährleistet ist. Dies gilt sowohl gegenüber dem Anbieter einer Software als auch gegenüber sonstigen Personen wie Familienangehörigen oder Besucherinnen und Besuchern beim Homeschooling.

Unabhängig von der technischen Ausgestaltung eines Dienstes (zum Beispiel durch die Verwendung einer Ende-zu-Ende-Verschlüsselung) kann die Vertraulichkeit gegenüber einem Anbieter durch die weitestgehende Vermeidung eines Personenbezuges hergestellt werden. So können für Chaträume etwa Pseudonyme vereinbart werden. Als Ersatz zum Präsenzunterricht reicht möglicherweise in manchen Fällen der Stream einer Präsentation mit Audiokommentar aus, ohne dass Schülerinnen und Schüler oder auch das Lehrpersonal zu sehen sind. Die Bereitstellung von Lehr- und Lernmaterial ohne Personenbezug über öffentlich verfügbare Dienste, etwa über eine Homepage, ist in jedem Fall aus Datenschutzsicht sich als unkritisch zu bewerten.

Die Schulen müssen beachten, dass zwischen ihnen und einem Dienstleister ein Vertrag zur Auftragsverarbeitung abzuschließen ist und dass Eltern vorab über die Datenverarbeitungsvorgänge (insbesondere im Verhältnis zum Anbieter) informiert werden. Sofern die Schule personenbezogene Daten von Eltern oder Schülerinnen und Schülern verarbeiten möchte, für deren Verarbeitung nicht bereits ein gesetzlicher Erlaubnistatbestand existiert (etwa private E-Mail-Adressen), ist dies nur auf der Basis einer Einwilligungserklärung der Eltern zulässig. Schülerinnen und Schüler ab 16 Jahren können diese Einwilligung selbst erteilen. In der Erklärung muss ein Hinweis darauf erfolgen, dass die Einwilligung freiwillig ist und Kinder keine Nachteile zu befürchten haben, wenn die Einwilligung nicht erteilt wird. Außerdem hat eine Belehrung hinsichtlich der jederzeit bestehenden Widerrufsmöglichkeit zu erfolgen.

Ein großer Diskussionspunkt ist der schulische Einsatz von Videokonferenzsystemen. Aus datenschutzrechtlicher Sicht ist hierbei der Einsatz von Software europäischer Anbieter, deren Server sich innerhalb des Geltungsbereichs der Datenschutz-Grundverordnung befinden, vorzugswürdig. Aber auch Open-Source-Lösungen, die Schulen oder Schulträger unter vollständiger eigener Kontrolle auf eigenen Servern oder auf Servern von Auftragsverarbeitern mit Standort innerhalb des Geltungsbereichs der Datenschutz-Grundverordnung betreiben, stellen eine Möglichkeit dar, den datenschutzkonformen Einsatz von Videokonferenzsystemen zu gewährleisten.

Bei der Nutzung außereuropäischer Videokonferenzsysteme durch Schulen ergeben sich hingegen verschiedene datenschutzrechtliche Probleme. Es lässt sich in aller Regel nicht verhindern, dass derjenige oder diejenige, der oder die unter Einsatz eines Softwareproduktes eines außereuropäischen Anbieters chattet, videotelefoniert oder Dokumente verschickt, beim Anbieter sogenannte Telemetriedaten hinterlässt. Telemetriedaten sind Daten, die sich nicht auf den Inhalt der Kommunikation beziehen, sondern auf deren Begleitumstände. Zu diesen gehören etwa die IP-Adresse, Informationen über die Dauer eines Gesprächs, Standortdaten und Angaben über das jeweilige Endgerät. Diese Daten werden dann an die Server des betreffenden Softwareanbieters übertragen, welche sich in aller Regel in sogenannten Drittländern befinden, also in Ländern, welche sich außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung befinden. Solche Übertragungsvorgänge sind nur dann zulässig, wenn auch hierfür eine legitimierende Rechtsgrundlage oder eine Einwilligung der betroffenen Personen vorliegt. Auf letztgenannte Möglichkeit können sich Schulen nicht berufen,

da die Datenschutz-Grundverordnung dies für den hoheitlichen Bereich ausschließt.

Besonders problematisch erweist sich seit dem Schrems-II-Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020 die Übermittlung von personenbezogenen Daten in die USA, da das Gericht in diesem Urteil den bis dahin bestehenden Angemessenheitsbeschluss, den sogenannten Privacy Shield, für ungültig erklärt hat. Der Privacy Shield steht also nicht mehr als Grundlage für die Übermittlung personenbezogener Daten in die USA zur Verfügung, sodass Verantwortliche auf andere Transferinstrumente zurückgreifen müssen.

Der Grund dafür ist vor allem darin zu sehen, dass Geheimdienste umfassende Zugriffsrechte auch auf Daten von Nicht-US-Bürgern haben, welche zum Beispiel bei der Nutzung von Software US-amerikanischer Anbieter auf deren Servern angehäuft wurden. Ihnen steht im Gegensatz zu US-Bürgern kein gerichtlicher Rechtsschutz gegen solche Maßnahmen zur Verfügung, um zu überprüfen ob und welche ihrer Daten gespeichert oder gar „durchleuchtet“ wurden. Dies betrifft eben auch Schülerinnen und Schüler, wenn sie zu Unterrichtszwecken beispielsweise Videokonferenzen durchführen.

Überhaupt sind viele Datenverarbeitungsprozesse bei US-Anbietern intransparent. Es ist etwa unklar und grenzt an Geheimniskrämerei, ob die Daten vom jeweiligen Anbieter auch für eigene Zwecke, etwa Werbezwecke, verwendet werden. Falls die jeweiligen Anbieter den Inhalt von Videokonferenzen zur Kenntnis nehmen oder gar speichern, eröffnet dies ein unüberschaubares Missbrauchspotenzial.

Im Ergebnis ist es für Schulen derzeit kaum noch möglich, rechtssicher Anbieter zu nutzen, bei denen Daten in die USA abfließen, da ihnen für die Datenübertragung faktisch keine Rechtsgrundlage zur Verfügung steht. Auch können die Schulen kaum ihrer nach der Datenschutz-Grundverordnung bestehenden Pflicht nachkommen, die Schülerinnen und Schüler zu informieren, was mit den erhobenen Daten passiert, denn aufgrund der Intransparenz der US-Anbieter und der unsicheren Rechtslage dort können die Lehrerinnen und Lehrer dies regelmäßig selbst nicht abschätzen.

Mit Blick auf die gegenwärtige pandemiebedingte Ausnahmesituation halte ich die vorübergehende Nutzung amerikanischer Videokonferenzsysteme daher nur dann für hinnehmbar, wenn folgende (hier auf Rheinland-Pfalz bezogene) Punkte beachtet werden:

- Bereits eingesetzte Lösungen US-amerikanischer Anbieter müssen auf schuleigenen Systemen betrieben werden oder es müssen, bei Inanspruchnahme eines Dienstleisters im Rahmen einer Auftragsverarbeitung gemäß Artikel 28 Datenschutz-Grundverordnung, die Konferenzdaten auf Systemen deutscher oder europäischer Anbieter verarbeitet werden. Zudem müssen die Lösungen datensparsam konfiguriert und mit von der Schule vergebenen, pseudonymisierten Zugangsdaten genutzt werden. Es muss eine Verwendung der Nutzungsdaten für Werbezwecke vertraglich ausgeschlossen werden (§ 103 Übergreifende Schulordnung Rheinland-Pfalz).

- Die Nutzerinnen und Nutzer müssen gemäß Artikel 13 Datenschutz-Grundverordnung informiert werden.

- Auf die in § 1 Absatz 6 Schulgesetz Rheinland-Pfalz vorgesehene Möglichkeit, eine verbindliche Nutzung digitaler Lehr- und Lernmittel vorzusehen, ist von den Schulen zu verzichten. Wenn Eltern, Schülerinnen oder Schüler einer Nutzung amerikanischer Softwareprodukte ausdrücklich widersprechen, müssen von Seiten der Schule und der zuständigen Lehrkraft äquivalente Lehrangebote zur Verfügung gestellt werden.

Meine Behörde hat mit Blick auf die Datenschutz-Herausforderungen zum Einsatz von Videokonferenzsystemen an Schulen mittlerweile verschiedene Erfahrungen gesammelt: Aus unserer Sicht ist es am sinnvollsten, wenn nicht jede Schule für sich selbst ein Videokonferenzsystem anschafft, konfiguriert und einsetzt. Weniger aufwändig und datenschutzrechtlich sicherer ist es, auf landeseinheitliche Systeme zu setzen, die von den jeweiligen Bildungsministerien zur Verfügung gestellt werden. In Rheinland-Pfalz hat sich etwa Big Blue Button (BBB), das auf Servern der Johannes Gutenberg-Universität Mainz gehostet wird, bewährt.

Gesundheitsdatenschutz an Schulen

Eine andere zentrale Fragestellung ist, wie Schulen mit Gesundheitsdaten umgehen. Im Jahr 2020 hat uns verstärkt beschäftigt, welche Informationen auf Attesten vermerkt sein müssen, die Schülerinnen und Schüler vorlegen, um keinen Mund-Nasen-Schutz tragen zu müssen. Wir haben darauf gedrängt, dass angesichts der besonderen Sensibilität von Gesundheitsdaten der Gesetz- oder Verordnungsgeber normenklar regelt, ob etwa Diagnosen auf den Attesten vermerkt sein müssen. In Rheinland-Pfalz ist die Landesregierung dem nachgekommen: Sie hat in der Corona-Bekämpfungsverordnung nunmehr für den Schulbereich den Umfang der Datenanforderung bei ärztlichen Attesten von Schülerinnen und Schülern und das Verbot der Anfertigung von Kopien ausdrücklich geregelt. Dies belegt aus meiner Sicht, dass das Recht auf informationelle Selbstbestimmung durchaus als gleichrangig mit anderen Grundrechten, wie dem Recht auf körperliche Unversehrtheit einschließlich der Gesundheit, angesehen werden kann.

Wenn Schülerinnen und Schüler in Präsenz unterrichtet werden, stellen sich zwei zentrale Fragen: Dürfen Schülerinnen und Schüler in den Schulen getestet werden? Wie ist mit den Testergebnissen umzugehen? Beides stellt in der Betrachtung des Alters der Kinder, der räumlichen Umsetzung sowie der Begleitung durch medizinisches Fachpersonal oder Lehrkräfte auch organisatorische und pädagogische Anforderungen an die jeweiligen Schulen.

Mit Blick auf Corona-Tests an Schulen ist zunächst zu unterscheiden, ob diese verpflichtend oder freiwillig durchgeführt werden. Wenn die Teilnahme auf freiwilliger Basis erfolgt, also nicht Voraussetzung für den Unterrichtsbesuch ist und keine weiteren Folgen an eine nicht erfolgte Testung geknüpft werden, stellt die Einwilligung die Rechtsgrundlage für die mit der Testung einherge-

henden Datenverarbeitungsvorgänge dar. Datenschutzrechtlich ist dies aus meiner Sicht nicht weiter problematisch.

Sollte der Schulbesuch nur gestattet sein, wenn eine Schülerin oder ein Schüler zuvor getestet worden ist, wenn also eine Testpflicht besteht, bedarf dies einer rechtlichen Grundlage. Diese kann sich unmittelbar aus Artikel 6 Absatz 1 Datenschutz-Grundverordnung in Verbindung mit konkretisierenden landesrechtlichen Regelungen der Corona-Bekämpfungsverordnung ergeben. Auch dann ist abzuwägen, ob eine Testung in der Schule erfolgen muss oder ob Selbsttests im häuslichen Umfeld oder in entsprechenden Teststationen und Apotheken als datenschutzkonformere Alternative in Frage kommen.

Bei Personen, die an Corona infiziert sind oder positiv getestet wurden, stellt sich die Frage, ob deren Namen anderen Schülerinnen und Schülern oder Lehrkräften gegenüber bekannt geben werden dürfen. Aus Gründen des Gesundheitsdatenschutzes sollte grundsätzlich keine Namensnennung erfolgen; zulässig ist aber die allgemeine und anonymisierte Nennung des Verdachtsfalls. Aus Fürsorgegründen zum Schutz von Risikogruppen oder wenn dies auf Bitte des Gesundheitsamtes für die Kontaktverfolgung erforderlich sein sollte, ist auch eine schulinterne Bekanntgabe unter namentlicher Nennung denkbar.

Der Nutzungsboom von Social Media und Messenger-Diensten

Bereits seit Längerem und auch bereits vor der Corona-Pandemie haben Schülerinnen und Schüler in ihrer Freizeit und zum Erledigen von schulischen Aufgaben immer häufiger und immer länger Social-Media-Angebote und Messenger-Dienste genutzt. Es ist seit Jahren ein Nutzungsboom von Web-2.0-Angeboten (Social Communities, Instant Messenger, Youtube, Wikipedia und anderen) zu verzeichnen. Neu hinzugekommen ist, dass zum Homeschooling viele dieser Dienste nun auch unterrichtlich und zur Kommunikation zwischen Schule und Lernenden sowie deren Eltern eingesetzt werden. Neben den Hausaufgaben via Messenger und Klassenchat oder Selbstlernen mittels Youtube-Tutorial erfolgt nun auch der Austausch mit den Mitschülerinnen und Mitschülern und das gemeinsame Bearbeiten einer Gruppenaufgabe digital und online über darauf spezialisierte Anbieter. Angesichts dessen gewinnt die digitale Bildung immer mehr an Bedeutung. Das Ziel aller Bildungsakteure sollte daher sein, dass die jungen Onliner und deren Eltern sensibilisiert werden, auf was sie bei der Nutzung von Web-2.0-Angeboten achten sollten. Folgende Fragen müssen dabei thematisiert und beantwortet werden: Welche Gefahren lauern im Netz? Wie sieht eine effektive digitale Selbstverteidigung aus? Welche Rechte können wem gegenüber geltend gemacht werden? Wie funktioniert das Geschäft mit Daten? An welchen Stellschrauben können und sollen Institutionen wie Schulen drehen, um den Datenschutz von Kindern und Jugendlichen zu verbessern?

Als Kooperationspartner des Landesprogramms „Medienkompetenz macht Schule“ leisten wir seit über zehn Jahren einen Beitrag zur digitalen Bildung in Rheinland-Pfalz. Als Teil dieses Programms veranstalten wir beispielsweise seit dem Jahr 2010 Schülerworkshops im ganzen Land, um Kinder und Jugendliche ab der dritten Klasse für einen sparsamen Umgang mit ihren Daten im Netz und mögliche Gefahren bei der alltäglichen Nutzung von Smartphone und Tablet zu sensibilisieren. Dieses Workshop-Programm haben wir durch Corona angepasst, denn auch ohne Präsenzunterricht müssen diese Inhalte auf anderen Wegen ihre Zielgruppe erreichen. Die Referentinnen und Referenten führen die Workshops daher inzwischen an einigen Schulen bereits als Online-Veranstaltungen durch, arbeiten didaktisch mit Online-Tools und thematisieren natürlich auch die neuen Lernumgebungen mit den Schülerinnen und Schülern. Dabei zeigt sich, dass sich rund um Online-Unterricht an den unterschiedlichen Schulen noch viele Fragen um die Verarbeitung von Daten stellen – sei es zur Wahl der Lernplattform oder die Frage, ob sich die Schülerinnen und Schüler vor der Kamera zeigen sollen und wie mit Störerinnen, Störern und Online-Trollen in der Videokonferenz umgegangen werden muss.

In Kooperation mit der Verbraucherzentrale bieten wir darüber hinaus Elternabende in Kitas an, um die Eltern möglichst früh auf die neuen digitalen Herausforderungen vorzubereiten.

Mit www.youngdata.de hat meine Behörde im Jahr 2013 speziell für Jugendliche eine Datenschutzseite entwickelt, die zwischenzeitlich als gemeinsame Jugendseite aller Datenschutzaufsichtsbehörden in Deutschland und des Kantons Zürich zielgruppengerechte Aufklärung im Bereich Datenschutz anbietet. Diese Seite werden wir im Laufe des Jahres komplett überarbeiten und optisch-funktional sowie auch inhaltlich noch stärker auf die Zielgruppe Jugendliche anpassen.

Aus Sicht des LfDI zeigt der Nutzungsboom, dass politische, staatliche und zivilgesellschaftliche Institutionen, Stellen und Vereine einen noch stärkeren Fokus auf die Medienbildung setzen sollten. Schülerinnen und Schüler sollen soweit wie möglich eine digitale Selbstständigkeit erlangen also lernen selbstständig IT-Produkte zu bewerten und auszuwählen. Das Ziel muss sein: Sie sollen die Hoheit über ihre Daten so weit wie möglich selbst ausüben. Sofern Bildungseinrichtungen auf Open-Source-Software wie Big Blue Button setzen, fördern sie damit auch die digitale Selbstständigkeit, Kreativität und Vielseitigkeit. Dies gilt in Pandemie-Zeiten, aber auch darüber hinaus.

Ausblick

Zusammenfassend kann festgehalten werden, dass die Pandemie den Datenschutz einem Stresstest unterzogen hat. Zum Teil ist die Debatte um die richtigen Maßnahmen gegen das Virus mit Blick auf den Datenschutz unsachlich und irrational geführt worden.

Allerdings ist es Deutschland bisher gut gelungen, auch in der Krise die Grundrechte nicht über Bord zu werfen und eine ausgewogene Abwägung zu treffen, ob und in welchen Fällen es notwendig ist, ein Grundrecht zu Gunsten eines anderen einzuschränken. Dass die Entscheidungsträgerinnen und Entscheidungsträger es sich damit nicht leichtmachen, ist gut so, denn diese Anforderung stellt ein freiheitlicher Rechtsstaat auch und gerade in Krisen-

zeiten. Dies sollten wir uns immer wieder bewusst machen. Ein angemessener Datenschutz darf dem Virus nicht zum Opfer fallen. Wir müssen den Datenschutz mit Vertrauen in sein differenziertes Funktionieren ausstatten und ihn vor haltlosen und pauschalisierenden Attacken schützen. Menschen lassen sich auf neue Technologien eher ein, wenn sie Vertrauen haben, dass ihre Rechte und Freiheiten gewahrt bleiben. Als Gesellschaft sollten wir seine wichtige Bedeutung anerkennen: Der Datenschutz ist kein Verhinderer, sondern ein wichtiger Regulator und Steuerungsfaktor.

Die Redaktion im Gespräch mit Dr. Lutz Hasse

Die Grundrechte dürfen nicht unter die Räder kommen!

Lutz Hasse ist im Jahr 2012 zum Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) bestellt und 2018 wiedergewählt worden. Ihn zu einem Gespräch zu bitten lag nah, da Herr Hasse die Arbeitskreise „Schulen und Bildungseinrichtungen“ sowie „Datenschutz- / Medienkompetenz“ der Datenschutzkonferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder (DSK) leitet.

Insoweit war es besonders interessant, seine Meinung zum Themenkomplex Datenschutz und Digitalisierung in der Bildung zu erfragen.

Frank Spaeing, Riko Pieper und Markus Eßfeld führten das Gespräch am 07.05.2021. Hier werden die Kernaussagen des Thüringer Landesbeauftragten wiedergegeben.[1]

Aufgabe und Rolle der Landesdatenschutzbeauftragten

In Deutschland gibt es insgesamt 18 unabhängige Datenschutzaufsichtsbehörden, da Bayern zwei und der Bund eine eigene Aufsichtsbehörde jeweils für ihre Zuständigkeitsbereiche haben sowie je eine Aufsichtsbehörde für die anderen Bundesländer.

Kernzuständigkeit ist es darauf zu achten, dass das Grundrecht der informationellen Selbstbestimmung geschützt wird. Die jeweilige Leitung der Aufsichtsbehörden ist Mitglied der Datenschutzkonferenz. Die Mehrheit der Mitglieder hat einen juristischen Ausbildungshintergrund. Die Meinungen gingen manchmal auseinander; das Bemühen um einen Konsens sei ausgeprägt. Ein gutes Beispiel sei die Task Force Schrems II, so genannt nach dem bekannten Urteil des Europäischen Gerichtshofs (EuGH). Der EuGH hat den Aufsichtsbehörden ins Hausaufgabenheft geschrieben, dass das Urteil zum internationalen Datentransfer (sogenanntes Schrems-II-Urteil) umzusetzen sei. Infolgedessen hat die Datenschutzkonferenz die Task Force Schrems II ins Leben gerufen, der auch Hasse angehört.

Dabei gehe es insbesondere darum, eine einheitliche Haltung der Aufsichtsbehörden herauszuarbeiten, etwa zu Datentransfers in die USA oder um die Rechtmäßigkeit der Nutzung von Software aus dem Hause Microsoft sicherzustellen, indem mit Microsoft Verhandlungen geführt werden.

Eine wichtige Aufgabe des TLfDI ist es außerdem pro Jahr ca. 26.000 Posteingänge von Bürgern, Institutionen, Behörden und Unternehmen zum Thema Datenschutz zu bearbeiten.

Die Zusammenarbeit mit den Aufsichtsbehörden anderer Bundesländer funktioniere in der Regel recht gut. Allerdings gebe es – bezogen auf den schulischen Bereich – keine durchweg gute Zusammenarbeit mit Kultusbehörden.

In Thüringen setze der TLfDI daher als oberste Datenschutzaufsichtsbehörde die Maßnahmen durch, die zum Grundrechtsschutz notwendig seien, auch wenn das nicht immer die Zustimmung des Kultusministeriums finde.

Als Beispiel aus dem schulischen Bereich nannte Hasse die Testung der Schüler auf Covid-19. Das sei eine Erhebung von Kinder-Gesundheitsdaten, die besonders schützenswert sind und daher den Einsatz des Landesbeauftragten erfordere.

Wenn der Hauptgeschäftsführer der bitkom, Bernhard Rohleder, behaupte, Datenschützer jagten einem Phantom hinterher, so müsse dies als abwegig bezeichnet werden.

Die in den jährlichen Tätigkeitsberichten von den Landes- und dem Bundesbeauftragten dargelegten zahlreichen Datenschutzverstöße, die nicht weniger zahlreichen Datenschutzskandale sowie die z. B. von Michal Kosinsky[2] gerade in den USA ermöglichten Profilbildungen und Verhaltensprognosen anhand von Aktivitäten in Sozialen Netzwerken sprechen deutlich eine andere Sprache.

Tätigkeit der Landesbeauftragten im schulischen Bereich

Vor dem Hintergrund des Schrems-II-Urteils kann die Nutzung von Microsoft 365 in den Schulen rechtswidrig sein. Teilnehmer der DSK sehen das unterschiedlich streng.

Hasse selbst hält es für möglich in Verhandlungen mit Microsoft vielleicht noch einen rechtskonformen Zustand erreichen zu können. Die DSK habe zur Klärung der amerikanischen Rechtssituation ein Gutachten in Auftrag gegeben, das den Fortlauf der Verhandlungen unterstützen bzw. begleiten soll. In jedem Fall sei es nicht Aufgabe der Schulen personenbezogene Daten in die USA zu liefern, was aber bei derzeitiger Nutzungspraxis von beispielsweise Microsoft-365-Produkten die Realität darstelle. Die DSK wird dann entscheiden, welche Maßnahmen nötig sind. Microsoft will Server-Farmen in Europa bauen, um die Situation zu entschärfen. Letztlich nütze das aber wenig, weil US-Behörden auch Zugriff auf europäische Server von Microsoft haben. Man müsse abwarten, ob juristische Konstrukte derartige Zugriffe vermeiden können.

Vorbehaltlich der erwähnten Entwicklungen möchte Hasse derzeit noch keine abschließende Stellungnahme abgeben.

Die DSK gebe abstrakte Hinweise zu Messenger-Diensten und Videokonferenz-Tools. Dass Schulleitungen datenschutzrechtlich Verantwortliche seien, sei nicht hilfreich, da in der Schule Tätige die datenschutzrechtlichen Fragestellungen mangels entsprechender Ausbildung kaum beantworten könnten.

Die kursorische Einschätzung einer Schul-App koste einen Informatiker seiner Behörde etwa einen Arbeitstag. Auf dieser Grundlage sind Thüringer Schulen mittlerweile durch seine Aufsichtsbehörde über 45 Apps informiert worden. Es gebe zudem eine Videokonferenz-Reihe. Zu jeder Konferenz werden 20 bis 30 Schulleiter geladen; sie würden zu Schuldatenschutzfragen informiert und anschließend würden Datenschutzprobleme diskutiert. Alles wird verschriftet und als FAQs ins Netz gestellt. Die Fragen zu den zu prüfenden Apps wiederholten sich mittlerweile, da habe man für die Schulleitungen inzwischen einen guten Grundstock erarbeitet.

Der Ruf nach einem „App-TÜV“ werde immer lauter, auch aus der Wirtschaft. Das sei auch absolut nachvollziehbar. Allerdings gebe es hier einige rechtliche und tatsächliche Hindernisse, an deren politischer Bewältigung er an vielen Stelle mitwirke.

Modellhaft etwa sei die Schul-Cloud des Hasso-Plattner-Instituts, Potsdam, entwickelt worden, nämlich unter Mitwirkung der Datenschutzaufsichtsbehörden. Dieses rechtzeitige Ziehen an einem Strang, um ein datenschutzkonformes Produkt zu entwickeln, sollte Schule machen. Privacy made in Germany sieht Hasse als Standortvorteil.

Insgesamt sei festzustellen, dass die Zusammenarbeit mit Schulen, Schülern und Eltern im Laufe der Zeit besser werde. Die Bedeutung des Grundrechts auf informationelle Selbstbestimmung wird zunehmend richtig eingeordnet.

Medienkunde-Unterricht

Das Bild ist eher düster. Die TU Ilmenau habe 2018 festgestellt, dass der Medienkunde-Unterricht in Thüringen stark defizitär sei. Eine entsprechende Ausbildung von Studenten und Referendaren fand überhaupt nicht statt. Heute hat sich zwar die Lehrerfortbildung verbessert, nicht genügend aber die Situation der Lehrerausbildung an den Hochschulen. Es fehle an Strategie und Systematik. Man müsse endlich anfangen! An der Basis wirkten sich Verbesserungen ohnehin erst in sechs bis acht Jahren aus. Man könne z. B. neue Lehrstühle schaffen. Es werfe Fragen auf, dass in der Volksrepublik China bereits Kita-Kinder Algorithmen programmieren können und in Deutschland nicht einmal Studenten diese Fähigkeit besäßen.

Auch die Evaluation der Lehrpläne sieht Hasse kritisch. Wenn man wirklich für das Leben und nicht für die Schule lerne, müsste im digitalen Zeitalter die ständige Fortentwicklung der Lehrpläne etwas Selbstverständliches sein. Und ja: Dafür könnten dann auch andere Lehrinhalte wegfallen.

Wenn behauptet werde, der Datenschutz hindere die Bildung, so sei dies einmal mehr blanker Unsinn. Tatsächlich würden viele Eltern dem TLfDI für seine Tätigkeit danken, auch im Zusammenhang mit dem oben erwähnten Datenerhebungsverfahren im Zusammenhang mit Covid-19, aber auch im Zusammenhang mit der schulischen Nutzung dubioser Videokonferenz-Systeme.

Verwendung von WhatApp

Die Verwendung von WhatsApp an Schulen in Thüringen ist verboten. Das Verbot wurde gemeinsam mit dem Kultusministerium ausgesprochen.

Tätigkeit des Arbeitskreises Schule, insbesondere Verhandlungen mit den Schulbuchverlagen

Auch mit den Schulbuchverlagen wurde und wird datenschutzrechtlich Relevantes erörtert. „Da sind wir noch nicht am Ende.“ Wenn ein Schüler sich beispielsweise bei der Hausaufgabenerledigung auf der Internet-Seite eines Verlages einlogge, würden sich Fragen stellen: Wie sind die Datenflüsse? Welche Daten werden erhoben? Was wissen die Verlage? Deswegen rede man mit den Verlagen und gemeinsam mit vielen Akteuren arbeite man an praktischen Lösungen.

Profiling

Art. 22 DSGVO treffe hier zwar Regelungen, die jedoch unzureichend seien.

Eine Regelung im BDSG, wonach eine Datenverarbeitung zum Zwecke eines Profilings meldepflichtig wäre, wäre sinnvoll, zumal es hier oft um Daten gehe, die wesentlich neuralgischer seien als diejenigen, die etwa bei der Nutzung von Videokameras anfielen. Auf diese Weise informierte Aufsichtsbehörden könnten dann gezielt prüfen, ob der Grundrechtsschutz eingehalten werde oder nicht.

Welche Medien werden zur Vermittlung von Wissen durch Schulen genutzt – gibt es Alternativen zu Youtube?

Youtube hat einen enormen Anteil am Unterrichtsgeschehen. Im AK Schule wird dieses Thema gerade erörtert. Zweifellos gebe es Datenabflüsse zu Youtube. Es sei, wie gesagt, nicht Aufgabe der Schulen Metadaten der Schüler in die USA abfließen zu lassen. Hinzu komme das Problem, dass Lehrer und Schüler häufig mit privater Computerausrüstung arbeiten müssten. Eigentlich müsste nach thüringischer Rechtslage der Lehrer dann vorab die Schulleitung fragen, ob er private Geräte im schulischen Kontext mit US-amerikanischer Software nutzen dürfe. Das müsste die Schulleitung dann eigentlich untersagen. Die Realität sehe aber wohl anders aus.

Überlegenswert erscheint Hasse der länderübergreifende Zugriff aller Lehrer auf die digitalen Lehrangebote aller anderen Bundesländer.

Hasse hat dies zum Thema in dem von ihm betreuten Arbeitskreis der DSK gemacht.

Planung der nächsten Jahre im Bereich „Bildung und Schule“

„Wir gehen nicht zurück auf Los.“ Nach der Pandemie sei es nicht wie vor der Pandemie. Digitalisierung und Schule werden keine Gegensätze mehr sein.

Auch virtuelle Realität und Künstliche Intelligenz sind dann irgendwann keine Fremdworte mehr für Schüler und Lehrer.

Die Landesbeauftragten sollten in diesem Entwicklungsprozess nicht nur als Aufsichtsbehörde gesehen werden, sondern gerade auch als Berater für alle sowie als Bündnispartner für Bildungsanbieter in Deutschland. „Daran werde ich weiter intensiv arbeiten."

Ausbildung in Sachen Datenschutz muss verpflichtend in die Ausbildungspläne für Lehrerreferendare aufgenommen werden.

Die Rolle der Kultusministerkonferenz mit ihren verbindlichen Strategiepapieren sollte nach Hasses Ansicht gestärkt werden – ein langer Weg.

Wie kommen die Aufsichtsbehörden ihrem Auftrag zur Sensibilisierung nach § 57 Abs. 1 Nr. 2 DSGVO nach?

Konkret hält Hasse (wie auch manche seiner Mitarbeiter) auf konkrete Einladung oder Initiative Anderer hin Vorträge zu Datenschutzthemen. Was vom TLfDI angeboten und auch regelmäßig angenommen wird, ist das Angebot von Praktika für Mitarbeiter von politischen Fraktionen. Auch Vorträge vor Fraktionen werden regelmäßig gehalten.

Als gesuchter Gesprächspartner von Medien transportiert Hasse aktuelle datenschutzrechtliche Themen, etwa zur Luca-App, Digitalisierung in der Schule, Covid-Daten im Schulbereich, usw.

Die Homepage des TLfDI enthält zahlreiche Hinweise, Links, Muster und Orientierungshilfen zur DSGVO allgemein oder auch speziell, z. B. für Schulen[3] und Unternehmen. Sehr gefragt ist seine Broschüre „Digitale Selbstverteidigung"[4].

Auch FAQ-Kataloge im schulischen und im unternehmerischen Bereich tragen zur Sensibilisierung bei, ebenso wie Vorträge in Schulen oder bei Industrie- und Handelskammern. Speziell für Schulen hat der TLfDI eine eigene Mediathek entwickelt, die Lehrangebote für Lehrer enthält, gegliedert nach den verschiedenen Klassenstufen.

Auch ein mit Hilfe der TU Ilmenau produziertes eigenes Lehrvideo zum Datenschutz erfüllt seine Funktion. Nachgefragt sind zudem die schulischen Fortbildungsveranstaltungen des TLfDI, z. B. zur Verschlüsselung oder Smartphone-Konfigurierung. Die stark nachgefragten Videokonferenzen mit den Schulleitungen zum Thema Schuldatenschutz wurden bereits erwähnt. An der Universität Jena hält Hasse Vorlesungen zum Datenschutz – unentgeltlich.

Hasse: „Unsere Öffentlichkeitsarbeit brummt, der Datenschutz ist inzwischen in Thüringen angekommen und die BürgerInnen wissen um die Bedeutung des Schutzes ihrer Privatsphäre und dass der TLfDI schlagkräftig an ihrer Seite steht."

1 Die Verwendung männlicher Sprache erfolgt im Interesse von Klarheit, Kürze und Einfachheit verbunden mit der Bitte, nicht das grammatische Maskulinum auf das biologische Geschlecht zu reduzieren. Zitate wurden jedoch nicht verändert.

2 https://taz.de/Psychologe-Michal-Kosinski/!5363681/

3 https://tlfdi.de/datenschutz/schule/

4 https://www.tlfdi.de/fileadmin/tlfdi/presse/digitale_selbstverteidigung_auflage_7_web.pdf



Bild: iStock.com/ skynesher

Bild: iStock.com

Jessica Wawrzyniak

Datenschutzfreundlicher Unterricht

Wo hakt es und welche guten Lösungen gibt es?

Ausgangslage

Die Wahl einer geeigneten digitalen Unterrichtsplattform war auch schon vor der Corona-Pandemie ein umstrittenes Thema. Doch der Zwang zum Fernunterricht und der quantitativ gestiegene Einsatz digitaler Werkzeuge zeigte schnell, wer in den letzten Jahren bereits in den Ausbau digitaler Bildung investiert hat, und wo die Digitalisierung von Schulen samt datenschutzrechtlicher Überlegungen eher stiefmütterlich behandelt wurde. Und mitten in diese Diskussion platzten im März 2020 die Schulschließungen durch die Corona-Pandemie. Hektisch wurden auf Städte- und Landesebenen Lizenzen für Videokonferenz-Programme wie Zoom oder Microsoft-Teams eingekauft und zur Verfügung gestellt. Zusätzlich wurden Dateiablagen bei Google Docs eingerichtet, Elterngespräche in Messenger wie WhatsApp ausgelagert oder auf umfassende digitale Unterrichtsumgebungen zurückgegriffen, wie Microsoft 365 oder Googles „G Suite for Education“ (um nur einige kritische Beispiele zu nennen)[1]. Dass diese Softwarelösungen etliche Schüler.innendaten sammeln und datenschutzrechtlich bedenklich sind, ist kein Geheimnis. Zur Beruhigung hieß es, dies seien Übergangslösungen und langfristig wurden geeignetere Programme in Aussicht gestellt. Doch letztere lassen auch nach über einem Jahr Distanzunterricht, und eigentlich seit zwanzig Jahren, noch immer auf sich warten – aus verschiedenen Gründen.

Jessica Wawrzyniak, Medienpädagogin im Verein Digitalcourage, erklärt, welche Hürden auf verschiedenen Ebenen die Umsetzung von datenschutzfreundlichem Unterricht erschweren, worauf es bei der Wahl von Schulsoftware ankommt und welche Alternativen bereits zur Verfügung stehen.

Die Rolle der Schülerinnen und Schüler

Datenschutzfreundlicher Unterricht wird zunehmend als Politikum behandelt, sodass der Kern des Themas in den Hintergrund gerät: Der Schutz von Kindern. Ihre Daten sind als wertvolles Gut zu betrachten, das vor wirtschaftlicher Ausbeutung geschützt werden muss, so legt es auch das Gesetz fest (ErwGr. 38 DSGVO). Die Erziehungspflicht von Eltern sowie der freiheitlich-demokratische Bildungsauftrag von Schulen sollen Kinder und Jugendliche auf dem Weg zur digitalen Mündigkeit unterstützen: Das Ziel sollte selbstbestimmtes, reflektiertes und eigenverantwortliches Handeln in der zunehmend digitalisierten Welt sein. Für Schülerinnen und Schüler ist es eine Lernaufgabe zu verstehen, welchen Wert ihre privaten Daten haben, in der Schule und in ihrer digitalen Freizeitgestaltung. Sie überblicken das große Ganze (z.B. wirtschaftliche und gesellschaftliche Zusammenhänge) erst mit steigendem Alter. Die Einschätzung, ob und wenn ja, welche Daten von ihnen verarbeitet werden dürfen, wird ihnen laut der Datenschutz-Grundverordnung erst ab 16 Jahren selbstbestimmt zugemessen (Art. 8 DSGVO) – vorher entscheiden i.d.R. die Erziehungsberechtigten darüber.

Eine 2018 vom Institut der deutschen Wirtschaft durchgeführte Studie zeigt: Zwei Drittel der befragten Kinder und Jugendlichen zwischen 14 und 21 Jahren weisen ein differenziertes und kritisches Bewusstsein für Datenschutz auf, doch die Ambitionen ihre Daten tatsächlich zu schützen, sind gering: Wenn zum Schutz der eigenen Daten auf einen beliebten Online-Dienst verzichtet oder sogar Geld in eine datensparsame Alternative investiert werden soll, wird auf diesen Schutz lieber verzichtet (Sozialforscher.innen sprechen dabei vom Phänomen „Privacy Paradoxon“).[2] Dass aufgeklärte Schülerinnen und Schüler sich im großen Stil gegen die Nutzung datensammelnder Software im Unterricht auflehnen, ist somit in naher Zukunft nicht zu erwarten, aber es ist auch nicht ihre Aufgabe. Ausnahmen bestätigen die Regel: In Baden-Württemberg setzt sich die Landesschüler.innenvertretung seit dem Herbst 2020 gemeinsam mit einem Bündnis aus verschiedenen Organisationen gegen Microsoft 365 und für Open-Source-Software im Unterricht ein.[3]

Die Rolle der Eltern

Also obliegt es den Eltern, auf den Datenschutz ihrer Kinder zu achten. Die Voraussetzungen für Medienkompetenz, Datenschutzwissen und Medienerziehung in Familien sind jedoch sehr divers. Neben dem Bildungsstand der Eltern, der Familiengröße und den finanziellen Ressourcen ist relevant, ob und wo Eltern sich zum Thema Mediennutzung und Datensicherheit informieren. Eine schweizerische Studie zeigte im Jahr 2019, dass ein Viertel der befragten Eltern Informationen zur Medienerziehung von der Schule ihres Kindes wünscht und somit auf die kompetente Einschätzung und Orientierungshilfe von Schulen vertraut[4]. Im Umkehrschluss ist davon auszugehen, dass Schulsoftware von Eltern weniger streng und kritisch beäugt wird als Apps und Dienste, die Kinder in der Freizeit und somit in ihrer direkten Obhut nutzen.

Welche Software in Schulen eingesetzt wird, liegt zwar nicht in der direkten Entscheidungsgewalt der Eltern, doch sie können den Auswahlprozess entscheidend lenken: Sie müssen um Zustimmung gebeten werden, wenn Daten von ihnen und ihren Kinder verarbeitet werden sollen (Recht auf informationelle Selbstbestimmung). Diese Zustimmung können sie auch verweigern. Insbesondere ist Vorsicht gebo-

ten, wenn Daten verarbeitet werden, die über notwendige Stammdaten hinausgehen, wenn externe IT-Dienstleister eingebunden werden, Daten an Dritte weitergegeben oder Programme eingesetzt werden, deren Datenverarbeitung sich der Steuerung durch die Schule entzieht. Davon sind somit mindestens der Einsatz aller Cloudlösungen, die Nutzung von Diensten außerhalb der EU, sowie der Einsatz proprietärer (nicht-quelloffener) Programme betroffen. Doch auch medienkompetente, aufgeklärte Eltern machen von dem Privileg des Widerspruchs selten Gebrauch. Sie möchten nicht als „Spielverderber" dastehen, die digitalen Unterricht torpedieren. Sie befürchten ihre latenten Sorgen nicht ausreichend fachlich begründen zu können oder sehen Nachteile für ihre Kinder, wenn diese von der Nutzung der Schulsoftware ausgeschlossen sind. Einige Eltern gehen bereits auf Schulen zu, verlangen Auskunft zur Verarbeitung der Daten (nach Art. 15 DSGVO), widersprechen der Nutzung von Software, reichen Beschwerden bei Landesdatenschutzbeauftragten ein und ein paar besorgte Mütter und Väter haben bereits einen juristischen Klageweg gewählt, um Schulen zum Einlenken zu bewegen.

Die Rolle der Schule (Leitung & Lehrkräfte)

Die Schulleitung trägt die Verantwortung für die Datenverarbeitung (§§ 120 bis 122 Schulgesetz NRW und Art. 28 der DSGVO). Sie steht dabei in einem ständigen Spannungsfeld zwischen den Vorgaben von Ministerien und Schulträgern, den administrativen Möglichkeiten vor Ort, individuellen Finanzierungsfragen und den Bedürfnissen von Schüler.innen, Lehrkräften und Eltern. Bei der Wahl der Schulsoftware werden datenschutzrechtliche Bedenken zudem häufig verdrängt, um den digitalen Unterricht überhaupt zu gewährleisten. Nicht aus Böswilligkeit oder weil beides zusammen nicht möglich wäre, sondern weil die Wirtschaft die Überforderung des Bildungssystemes ausnutzt und schnelle, einfache Lösungen anbietet: Die Angebote von datensammelnden IT-Großkonzernen stehen ohne langen Vorlauf zur Verfügung, halten hohe Auslastungen aus und beinhalten technischen Rund-um-Support – genau das, was Schulen zur Entlastung brauchen.

Dabei ist es gar nicht so einfach, wie es auf den ersten Blick aussieht: Die Schulleitung hat den Betroffenen gegenüber eine umfassende Auskunftspflicht darüber, welche Daten verarbeitet werden, für welche Zwecke, wo und wie lange diese gespeichert werden, usw. (Art. 15 DSGVO). Um diese Informationen vom externen Datenverarbeiter zu bekommen, muss die Schulleitung einen Auftragsverarbeitungsvertrag (AVV) mit dem externen Datenverarbeiter (z.B. Microsoft) abschließen, in dem der Umgang mit den Daten detailliert geklärt und zudem hinreichend garantiert wird, dass kein Schaden für die Nutzer.innen entsteht. Die Schulleitung entscheidet, ob sie den Vertragsinhalten glaubt und zustimmt – auf eigene Verantwortung (Art. 28 DSGVO). Und schon ist die Lage komplexer als angenommen, denn wenn sie ehrlich sind, müssen Schulen zugeben, dass sie viele Fragen zur Datenverarbeitung nicht sicher beantworten können, wenn sie proprietäre (nicht-quelloffene) Software aus Nicht-EU-Ländern verwenden, z.B. von Microsoft, Google oder Apple. Gleichzeitig ist der Druck eine Lösung für digitales Lernen zu finden, so groß, dass das Recht auf Bildung und das Recht auf informationelle Selbstbestimmung gegeneinander abgewogen werden. Und zu oft wird dabei vergessen, dass Grundrechte nicht verhandelbar sind.

Lehrkräfte, die ebenfalls von der Verarbeitung ihrer Nutzerdaten betroffen sind, wenn auch in unkritischerem Maße als die Kinder, können wie alle anderen Bürgerinnen und Bürger von ihrem Recht auf informationelle Selbstbestimmung Gebrauch machen. Allerdings spielen an der Stelle arbeitsrechtliche Bedingungen mit rein, u.a. die Erfüllung des Lehrauftrags. Verbeamtete Lehrkräfte haben im Zuge des Remonstrationsrechts die Möglichkeit, fragwürdige Weisungen ihres Vorgesetzten in Frage zu stellen, z.B. die ausschließliche Nutzung einer grundrechteverletzenden Software, und von der nächst höheren Dienstposition prüfen zu lassen.[5]

Grundsätzlich muss die Schule alternative Möglichkeiten zur Partizipation am Unterricht schaffen, wenn Schüler.innen oder Lehrkräfte der Nutzung eines Programms widersprechen. Den Betroffenen dürfen keine Nachteile entstehen, sodass die Zustimmung zur Datenverarbeitung unter keinen Umständen ihre Freiwilligkeit verliert (ErwGr. 43 DSGVO).

Die Rolle der Politik

Auf Ebene der Länder, Städte und Kommunen werden permanent Lösungen für Schulen vorgeschlagen und entsprechende Mittel bereitgestellt. Einige haben sich bereits auf den Weg mit datenschutzfreundlicher, freier Software gemacht, aber an vielen Stellen besteht Nachholbedarf. So kommt es immer wieder zu Fällen, in denen einzelne Schulen die Nutzung von datenschutzfreundlichen Programmen wünschen, städtische Mittel jedoch für Lizenzen, z.B. von Microsoft, ausgegeben werden, um zugleich auf eine gut ausgebaute Support-Struktur zurückgreifen zu können. Ministerien investieren in den Ausbau datensammelnder Software, wie z.B. in Baden-Württemberg, wo 2020 Microsoft 365 in Pilotprojekt-Schulen eingeführt wurde[6]. Letzlich ist die Umsetzung der digitalen Bildungsplattform mit Microsoft-Software von der Landesdatenschutzaufsichtsbehörde gestoppt worden, doch wer das Software-Paket bereits verwendet hat, muss sich nach den Sommerferien 2021 wieder einmal neu aufstellen.[7]

Solche Rückschläge führen zu Zweifeln gegenüber den vorgeschlagenen Lösungen und zwingen Bildungseinrichtungen dazu ggf. ihre eigene Digitalisierungsstrategie umzusetzen. Wer in solchen Fällen keinen zahlungskräftigen und eigenmächtig handelnden Schulförderverein hinter sich hat, befindet sich in einer Sackgasse. Da der Schutz von Schüler.innen-Daten bei der Verwendung von „intransparenter Software" immer wieder angezweifelt wird, muss die Politik den Ausbau von Open-Source-Projekten in der EU besser fördern – mit finanziellen Mitteln und attraktiven Anreizen für Schulen (z.B. gute Support-Struktur und Weiterbildungen für Lehrkräfte). So lange Schulen die „Katze im Sack" kaufen müssen und ihre Verantwortung für die Datenverarbeitung von einem schlechten Gefühl begleitet wird, kann Datenschutz

nicht seine negative Konnotation des notwendigen Übels verlieren. Den Mehrwert von Datenschutz zu vermitteln muss ebenfalls seitens politischer Programme verstärkt werden.

Was macht heimische Open-Source-Software attraktiv?

Nur Programme, die der Europäischen Datenschutz-Grundverordnung (DSGVO) unterliegen, können vom deutschen Rechtssystem umfassend abgedeckt und unserem Verständnis von gutem Datenschutz gerecht werden. Zudem können offene Quellcodes besser sichern, dass Datenflüsse erkannt und unterbunden werden können. So genannte „freie Software“, die sich nicht nur durch einen öffentlich einsehbaren Quellcode auszeichnet, sondern auch lizenzfrei zur Verfügung steht, kann von allen Entwickler.innen genutzt und weiterentwickelt werden, um bestmögliche und kreative Softwarelösungen zu schaffen. Um Monopolstellungen von Unternehmen entgegenzuwirken, aber auch zum Schutz bei Serverausfällen oder vor Datenverlust, ist es von Vorteil Daten dezentral zu speichern z.B. auf Servern in den Rechenzentren der Städte. Die Nutzung freier oder quelloffener Software ermöglicht es zudem das Bildungssystem unabhängig von kommerziellen Interessen zu halten und den Bildungsauftrag zu erfüllen, der auf freiheitlich-demokratischen Werten basiert. Der Einsatz von „Marken-IT“ bindet Schülerinnen und Schüler von klein auf an die gesamte Produktpalette des Anbieters und beeinflusst die Entfaltung der Persönlichkeit: Die permanente Zufuhr von Nutzungsdaten und persönlichen Informationen ermöglicht differenzierte Persönlichkeitsanalysen, macht schon junge Kinder zu gläsernen Menschen, angreifbar und manipulierbar. Für Schulen, die sich u.a. als Schutzraum für Heranwachsende verstehen, sollte Open-Source-Software der Mindeststandard sein.[8]

Welche Möglichkeiten gibt es bereits?

Allgemeine Schul-IT: Eigens für Schulen angepasste Netzwerke wie Skolelinux/DebianEDU oder Linuxmuster statt Windows-Betriebssystemen machen möglich die gesamte IT-Infrastruktur auf freie Softwarelösungen umzustellen. Mit einer Ausnahme: Die von den Ministerien zur Verfügung gestellte Schulverwaltungssoftware zur Kommunikation zwischen Schulen und Aufsichtsbehören steht selten für Linux zur Verfügung. Das sollte sich dringend ändern.

Unterrichtsumgebung: Moodle ist ein Lernmanagement-System, das kommerziellen Plattformen kaum nachsteht. Unterrichtsmaterialien, Hausaufgaben, Tests und Lernfortschritte sowie kollaboratives Arbeiten von Lerngruppen kann dort digital umgesetzt werden. In Moodle lässt sich auch die Videokonferenz-Software „BigBlueButton“ integrieren.[9] Eine weitere Möglichkeit, sich während des Unterrichts zu sehen, bietet „Jitsi“ (oder das für Schulen angepasste „Meetzie“[10]). Eine Dateiablage ist zwar in Moodle bereits enthalten, doch mit „Nextcloud“ stehen zusätzlich noch ein Terminkalender und ein Kanban zur Verfügung. Nextcloud-Talk bietet auch die Möglichkeit zu „videokonferieren“. Eine Art digitales Klassenbuch (Noten, Fehlzeiten, Stundenpläne, usw.) bietet z.B. „GradeMan“ (für diese besonders sensiblen Daten sollten allerdings analoge Lösungen immer bevorzugt werden).

Werkzeuge: Für das Erstellen von Texten, Tabellen und Präsentationen eignen sich „Libre Office“ oder „Collabora“. Wer gemeinsam schreiben möchte, kann „Etherpads“ oder „Cryptpads“ dafür nutzen. Letztere bieten auch eine übersichtliche Ordnerstruktur zum Ablegen der Dokumente. Für sämtliche weiteren digitalen Tätigkeiten, die im Unterricht relevant werden, gibt es ebenfalls freie Lösungen. So können z.B. Bilder mit „GIMP“ bearbeitet werden, Musik mit „Audacity“ und Videos mit „OpenShot“. Das Lernen an sich kann von Programmen wie „Anki“ (Karteikarten) oder „Freemind“ (Mindmaps) unterstützt werden. Software für den fächerspezifischen Unterricht, vom Vokabeln-Lernen bis zum Noten-Schreiben ist sehr vielfältig verfügbar. Auskunft geben beispielsweise Websites zu OER-Materialien (Open Educational Ressources), wie oer.schule oder medien-in-die-schule.de[11].

1 Datenfresser an Schulen: https://digitalcourage.de/blog/2020/datenfresser-an-schulen

2 Studie des Instituts der deutschen Wirtschaft: https://www.iwkoeln.de/studien/iw-trends/beitrag/barbara-engels-datenschutzpraeferenzen-von-jugendlichen-in-deutschland.html

3 Bündnis „Unsere digitale Schule“: https://unsere-digitale.schule/

4 MIKE-Studie 2019: https://www.zhaw.ch/de/psychologie/forschung/medienpsychologie/mediennutzung/mike/#c145075

5 https://www.gew-nrw.de/remonstration.html

6 Laudatio bei den BigBrotherAwards 2020: https://bigbrotherawards.de/2020/digitalisierung-bildungsministerin-baden-wuerttemberg-susanne-eisenmann

7 Warnung des LfDI: https://bnn.de/nachrichten/baden-wuerttemberg/warnung-datenschutzbeauftragter-microsoft-office-365-schulen-baden-wuerttemberg

8 Freie Software für Schulen: https://digitalcourage.de/blog/2020/freie-software-fuer-schulen

9 BigBlueButton in Moodle: https://blog.hwr-berlin.de/elerner/anleitung-zur-nutzung-von-bigbluebutton-auf-moodle/

10 Meetzie: https://klassenzimmer.meetzi.de/

11 Achtung, das Projekt wird u.a. von Google gefördert. Die Software-Empfehlungen sind jedoch größtenteils quelloffen.



Beispiele für freie Software

Thomas Freihorst, Steffen Haschler, Benjamin Schlüter

Schule digital: Wie ein Lock-In an Schulen der Gesellschaft schadet

Was kurzfristig den Unterricht sichern soll, wird langfristig negativ auf unsere Bildung und unsere Gesellschaft wirken. Chaos macht Schule zeigt Auswege.

Dieser Artikel ist so bereits am 09.04.2021 auf heise.de erschienen und wird mit freundlicher Genehmigung hier abgedruckt.[1]



Bild: shutterstock.com/Black Jack

Überstürzt wurden in den vergangenen Wochen und Monaten an Schulen neue Geräte und Software angeschafft, um in der Coronavirus-Pandemie Distanzunterricht oder auch Hybridunterricht zu ermöglichen. Doch was den Unterricht während der Pandemie schnellstmöglich sichern sollte, wird auf lange Zeit negative Auswirkungen auf unser Bildungswesen und unsere freiheitlich-demokratische Gesellschaft haben. Wir verschärfen dadurch den Lock-In-Effekt. Aber was ist der Lock-In-Effekt eigentlich?

Der Lock-In-Effekt

Der Begriff des Lock-In-Effekts[3] stammt aus der Betriebswirtschaft und den Wirtschaftswissenschaften. Ein Lock-In bindet Kund:innen an ein bestimmtes Produkt, weil sich ein Wechsel zu einem Konkurrenzprodukt wirtschaftlich nicht lohnt. Erreicht wird dies durch fehlende Interoperabilität zwischen den Produkten. Klassische Beispiele dafür sind Rasierklingen oder Objektive für Fotokameras, die nur mit den Produkten eines einzelnen Herstellers kompatibel sind.

Um Kund:innen für diese Abhängigkeiten zu gewinnen, werden sie zumeist mit attraktiven Startangeboten gelockt. Die Folgekosten werden bei Kaufentscheidungen selten mitkalkuliert. Langfristig profitieren daher die Hersteller von der Bindung mehr als die Kund:innen. Solche Lock-In[4]-Bindungen gibt es im Informationszeitalter natürlich auch bei Hardware- und Software-Produkten.

Unbewusst Weichen für die Zukunft gestellt

Wenn gerade Technologien an Schulen überhastet eingeführt werden, möchten die Bildungsverantwortlichen nur sicherstellen, dass Distanzunterricht in Zeiten der Pandemie stattfinden kann, bevor die Schulen in nicht allzu ferner Zukunft wieder zum klassischen Unterricht – also dem analogen Präsenzunterricht – zurückkehren können. Tatsächlich vollziehen die Schulen dabei unbemerkt eine überstürzte Transformation vom Industriezeitalter zur Informationsgesellschaft, bei der Entscheidungen getroffen werden, die aufgrund von Lock-In-Effekten nur mit hohen Kosten und viel Mühe rückgängig gemacht werden können.

Viele Technologiefirmen sehen gerade in der Pandemie eine echte Chance in die Bildungseinrichtungen drängen zu können, preisen deshalb offensiv ihre Lösungen an und bieten sogar direkte Hilfe für die Erstellung von Medienentwicklungsplänen[5]. Dabei haben viele dieser Firmen in der Vergangenheit bereits Produkte an Schulen verkauft, die sich als nicht praxistauglich erwiesen haben, wie zum Beispiel die interaktiven Tafeln der Firma SMART. Dem hohen Absatz lag ein gutes Marketing zugrunde und kein stimmiges Konzept für Schulen[6].

Solchen Firmen ist es wichtiger ihre Produkte zu verkaufen, als dass ein nachhaltiges und passgenaues Medienkonzept für eine Schule entsteht. Dass solche Angebote dennoch gerne von Entscheider:innen angenommen werden, liegt daran, dass es ihnen an informatischen Fachkenntnissen, an pädagogisch-didaktischer Erfahrung oder an Zeit fehlt – meistens sogar an allem, denn die digitale Transformation der Schulen wurde über Jahrzehnte verschleppt[7].

Schulen sind besonders anfällig für Lock-Ins

Lock-In-Effekte gab es im Schulsystem natürlich schon immer. Schließlich sind Schulen Orte, zu denen nur wenige Dienstleister wie beispielsweise Schulbuchverlage Zugang erhalten. Denn mit Einführung eines bestimmten Schulbuches wird das Curriculum des Faches mit festgelegt und Lehrkräfte erstellen passend dazu Arbeitsblätter, Klausuren und mehr. Das festigt die Bindung an das Buch weiter. Die Geschäftsmodelle dieser Dienstleister sind auch auf den Erhalt dieser Exklusivität ausgerichtet und erschweren so Innovation. Bei den Schulbüchern wird unter anderem mit entsprechenden Lizenzen die Entstehung von freien Bildungsmaterialien, die auf den Lernplattformen dringend gebraucht werden, erschwert.

Der sich jetzt abzeichnende Technologie-Lock-In in Schulen wird allerdings deutlich stärker ausfallen als die seit Jahrzehnten bestehenden Lock-In-Probleme wie bei dem oben erwähnten Schulbuch. Nicht nur bilden sich langfristige Abhängigkeiten aus, sondern die angeschafften Techniklösungen prägen neben den Lehrplänen für eine lange Zeit auch die Einstellungen ihrer Nutzer:innen.

Lock-In bei Hardware

Die Lock-Ins durch neu angeschaffte Hardware zeichnen sich bereits in vielen Städten ab. Denn sie setzen für ihre Schulen vermehrt auf Tablets wie das iPad von Apple[8]. Gute Gründe gibt es: Die Geräte sind robust und durch ihr abgeschlossenes Betriebssystem können Nutzer:innen wenig kaputt machen. Grundschulen schätzen an iPads, dass diese einfach zu bedienen sind und die iOS-App-Welt gut gemachte Anwendungen für ihren Unterricht bereithält. Da es sich bei Apple um eine begehrte Marke handelt, nutzen Schulträger diese auch gerne als Werbung für ihre Schulen[9].

Dass das Betriebssystem ziemlich abgeschottet ist und jegliche Logik von Datei- und Ordnerstrukturen versteckt, womit das Gerät zu einer smarten Blackbox wird, spielt für sie nur eine untergeordnete Rolle. Dies ändert sich mit dem Alter der Schüler:innen. Da sich Schulen aber als Ganze für einen Endgerätetyp für ihre Lehrkräfte entscheiden müssen[10], sind die Schwierigkeiten im Kollegium vorprogrammiert, wenn zum Beispiel eine Lehrkraft einen Laptop mit einem freien Betriebssystem möchte.

Lock-In scheint attraktiver als Aufbau von Know-how

Einige Schulträger gehen noch einen Schritt weiter und nehmen zusätzlich Produkte wie AppleTV direkt in ihren Medienentwicklungsplan auf (Siehe etwa die Stadt Hannover, 1000-2020, 2754-2020)[11]. Durch solche Maßnahmen werden andere Endgeräte systematisch ausgeschlossen und Umgebungen etabliert, welche die Handlungsmöglichkeiten der Lehrkräfte stark einschränken. Für einen späteren Kurswechsel müsste die angeschaffte Infrastruktur in Teilen ausgetauscht werden und es würde wiederum eine Einarbeitung in ein neues System stattfinden müssen. Dies trifft natürlich auch auf die Expertise der IT-Abteilung des Schulträgers zu, die nur einseitig auf ein bestimmtes System trainiert wird.

An den meisten Schulen fehlen immer noch Vollzeit-Administrator:innen. Einerseits werden diese Stellen für Schulen von den Kommunen gar nicht erst geschaffen, andererseits sind diese bei IT-Fachkräften finanziell gesehen häufig nicht konkurrenzfähig[12]. Dies führt dazu, dass von unterdimensionierten kommunalen IT-Abteilungen einfache Lösungen bevorzugt werden, die mit dem bestehenden Personal umgesetzt werden können. Es werden beispielsweise einfach bedienbare Mobile-Device-Management-Systeme eingeführt, die aber nur eine Monokultur wie iPads ermöglichen[13]. Wie so oft wird Geld nicht in eigenes Personal, sondern in Lizenzen internationaler Konzerne investiert.

Klare Kriterien verhindern Hardware-Lock-In

Um nicht in die Gefahr eines Hardware-Lock-Ins zu laufen, muss die Infrastruktur eine Diversität an Endgeräten zulassen. Als Faustregel sollte gelten: Hardware und Software müssen voneinander unabhängig betreibbar sein. Dadurch wird das gesamte System flexibler und somit resilienter – Veränderungen werden leichter umsetzbar. Es gibt mehrere Schulen in Deutschland, die sich hierbei auf einem sehr guten Weg befinden, wie zum Beispiel das Georg-Büchner-Gymnasium Seelze nahe Hannover[14], das den Weg einer Linux-Schule geht und eine nachhaltige Digitalisierung anstrebt[15].

Generell sollte bereits bei der Wahl der Hardware in Schulen auf Fragen wie „Wer macht was mit meinen Daten?“ und auf Reparierbarkeit beziehungsweise den Umweltschutz insgesamt geachtet werden. Hier fehlt es an klaren Vorgaben seitens der Ministerien, obwohl einige Länder bereits pro Klima handeln möchten. In der Verfassung von Niedersachsen steht beispielsweise: „In Verantwortung auch für die künftigen Generationen schützt das Land das Klima und mindert die Folgen des Klimawandels.“[16]

Mit in die Auswahl der Endgeräte sollten auch Themen wie Konfliktmaterialien, Menschenrechtsverletzungen, Kinderarbeit einfließen[17]. Denn auch Schulen haben als Teil unserer Gesellschaft eine Verantwortung gegenüber den künftigen Generationen, wie es immer wieder von Fridays for Future gefordert wird[18].

Lange Gerätezyklen sparen Kosten und Ressourcen

Zur Auswahl der Endgeräte gibt es unsererseits Empfehlungen[19]. Bei Tablets hat sich ein Herstellersupport für das Betriebssystem von längstens 5 Jahren etabliert[20]. Diesen Zyklus gibt meist nicht die eigentliche Hardware vor, sondern der Hersteller und so wird nach dieser Zeit trotz intakter Hardware ein neues Tablet angeschafft. Felix Schoppe, Lehrer am Georg-Büchner-Gymnasium, berichtet dazu: „Wir leben digitale Nachhaltigkeit vor. Wir installieren und reparieren unsere Laptops zusammen mit Schülerinnen und Schülern und zeigen, dass man selbst zehn Jahre alte Business-Notebooks noch aktiv einsetzen kann. In Verbindung mit GNU/Linux verleiht man so vermeintlichem Elektroschrott ein neues Leben.“

Dabei geht es nicht darum, bestimmte Endgerätegruppen aus unseren

Schulen zu verbannen. Eine Schule könnte Endgeräte mit GNU/Linux besonders fördern, aber allen am Schulleben Beteiligten trotzdem die Wahl selbst überlassen. Zudem werden Spezialgeräte wie Grafiktablets für das Fach Kunst oder Festrechner für die Informatik vorgehalten.

Kreativ mit Personalmangel umgehen

Für die Umsetzung eines solchen Szenarios bedarf es natürlich entsprechender Ressourcen. Computer-AGs können die Schul-IT unterstützen und sich sogar an der Weiterentwicklung von freier Software[21] beteiligen. Dies wird von einigen Schulen, wie dem Katharineum aus Lübeck[22] schon seit Jahren erfolgreich praktiziert, wie der stellvertretende Schulleiter Frank Poetzsch-Heffter berichtet: „In der Arbeit der Computer AG sehe ich eine Win-Win-Situation: Einerseits fördern wir Begabungen bis hin zu Kontakten in den Profibereich, andererseits erhalten wir wichtige Impulse für die Wartung und Verbesserung der IT-Technik."

Zusätzlich bedarf es ausgebildeter Techniker:innen, die den Schulen zur Verfügung stehen, wenn es um Grundsätzliches geht. Des Weiteren können Schulassistent:innen für den First-Level-Support ausgebildet werden und es könnte ein Freiwilliges Technisches Jahr an Schulen etabliert werden, auch für ältere Menschen, die aus ihren Berufen mit viel Fachwissen ausscheiden.

Lock-In bei Software

Bereits das oben angesprochene großflächige Anschaffen von iPads bringt Schulen einen zusätzlichen Software-Lock-In ein. Aber nicht nur auf Ebene der Betriebssysteme gibt es Lock-In-Fallen für unsere Schulen, denn wie in jedem Unternehmen sind dort eine Vielzahl unterschiedlicher Programme im Einsatz. Es gibt Verwaltungssoftware wie ein Notenprogramm, ein digitales Klassenbuch oder spezielle Software für den Fachunterricht. Außerdem werden in der Pandemie kurzfristig viele Lernplattformen eingeführt, auf denen sich neben Unterricht auch der Austausch des Kollegiums organisiert.

Software-Anschaffungen gefährden digitale Souveränität

Für die Auswahl von für den Unterricht zugelassener Software existieren bisher wenige Vorgaben vonseiten der Ministerien. Das überrascht, da beispielsweise Schulbücher vor deren Einsatz ein Prüfverfahren durchlaufen. Und so wird rechtswidrige Software wie Microsoft Teams von Schulträgern ausgewählt.

Dass nach jahrelangem Hin und Her für Microsoft Teams ein Verbot ab dem 1. August für hessische Schulen ausgesprochen wurde[23], kommt sehr spät für viele Schulen. Die Politik hätte dies deutlich früher vorgeben müssen. Denn nicht Landesdatenschutzbeauftragte, sondern Gesetze geben vor, was erlaubt ist und was nicht. Ein Grund für das nötige Verbot ist, dass sich bei der Nutzung von Teams Daten beim US-Konzern ansammeln. Ein „Recht auf Vergessenwerden" ist nicht gewährleistet[24] und die digitale Souveränität unserer Schüler:innen[25] somit gefährdet.

Zu starke Bindung an Software ist teuer

Neben den Problemen beim Einsatz von Teams die Datenschutzgesetze einzuhalten, ist ein Lock-In in der von Microsoft erdachten Bildungswelt[26] vorprogrammiert. Denn Teams lässt keinen einfachen Datenexport oder -import zu, nutzt proprietäre Formate, ist wenig anpassbar und lässt sich schlecht mit anderen Anwendungen kombinieren. Dies bekommen viele öffentliche Schulen in Hessen, die seit Langem auf Teams setzen, nun zu spüren: Weder lassen sich dort erstellte Klassenteams in einer neuen Lernplattform importieren, noch können über Jahre gewachsene Class Notebooks[27] oder in Forms erstellte Quizze aus Teams weiter genutzt werden. Diese Problematik addiert sich dann noch ungünstig mit dem immer bestehenden Schulungsaufwand aller Nutzer:innen auf neue Produkte, wofür im ohnehin stressigen Schulalltag wenig Zeit ist – insbesondere nicht während einer Pandemie. Gäbe es das behördliche Verbot in Hessen nicht, würden sicherlich die meisten der betroffenen Schulen bei Teams bleiben.

Pädagogik und Didaktik haben Vorrang vor Technik

Wegen der fehlenden Anpassbarkeit und dem schwierigen Datenexport aus proprietärer Software sollten auch datenschutzkonforme Lösungen wie its learning[28] nicht in unseren Schulen verwendet werden. Vergleicht man die Welt von vor zehn Jahren mit der heutigen, wird klar, dass wir nicht wissen, welche Technologien in weiteren zehn Jahren in Schulen gebraucht werden. Geschlossene Systeme sind zu unflexibel; sobald sie nicht mehr zu den eigenen Bedürfnissen passen, sitzt man in der Lock-In-Falle. Zu beobachten war dies zu Beginn der Pandemie, als das Videokonferenztool von Teams noch nicht über Breakout-Räume verfügte. Den Lehrkräften und Schüler:innen blieb nur das Verzichten auf Gruppenarbeiten und ein Warten auf das entsprechende Update. Somit musste sich Pädagogik und Didaktik nach der Technik richten anstelle umgekehrt bei gleichzeitiger Einnahme einer passiven Konsumentenhaltung, welche die digitale Mündigkeit gefährdet[29].

Und wer weiß heute, ob OneNote eines Tages eingestellt wird oder ob ein Unternehmen pleitegeht? Wenn Lehrkräfte ihr gesamtes Material in solchen geschlossenen Systemen erstellen, könnte das ein echtes Problem werden. Das haben die Nutzer:innen von „Padlet", einer digitalen Pinnwand, im vergangenen Jahr gemerkt. Das Tool erfreute sich großer Beliebtheit bis es kostenpflichtig wurde und man seine Datenschutzprobleme aufdeckte. Viel Material und viele Arbeitsstunden gingen verloren.

Mit freier Software und Kooperation den Lock-In verhindern

Das sich monatelang hinziehende Drama um Teams hätte man den Schulen ersparen können[30], wenn man von vorneherein auf bereits bestehende und praxiserprobte freie Technik gesetzt hätte. Eine solche ist zum Beispiel das seit Jahren betriebene BelWü-Hochschulnetz. Im eigens für den Unterricht in Baden-Württemberg angepassten Moodle[31] wurde in kurzer Zeit und von wenigen Freiwilligen ein Videokonferenzsystem für Schulen hinzugefügt,

als es zu Schulschließungen kam[32], was die Fähigkeit der Anpassung freier Software verdeutlicht. Dass die Systeme anfänglich teilweise unter Last zusammenbrachen, ist nachvollziehbar angesichts der Unterfinanzierung und den Ausstattungsmängeln, mit denen teilweise bis jetzt gekämpft wird. Diese Anpassung braucht es aber, um für jede einzelne Schule individuelle Lösungen bereitstellen zu können. Die technische Umsetzung kann überregional vorbereitet werden und Schulen können sich dann die Teile installieren, die sie wirklich brauchen.

Eine länderübergreifende Entwicklung spart dabei nicht nur Kosten, sondern hilft beim Beheben von Sicherheitslücken und anderer Softwarefehler. Sie setzt allerdings voraus, dass erfolglose Alleingänge, wie wir sie bei den Lernplattformen beobachtet haben[33], durch kooperatives Handeln ersetzt werden. Dabei braucht es offene Schnittstellen nicht zuletzt auch, um Lernenden und Lehrenden bei einem Schulwechsel einen einfachen Umzug ihrer Daten zu ermöglichen und neue Lernwerkzeuge einfach integrieren zu können.

Die eingesetzte Software muss quelloffen vorliegen, damit Interessierte in der Lage sind sie zu verstehen, zu bewerten und zu hinterfragen. Wird eine solche Installation dezentral betrieben, werden Schulen digital souverän: Die einzelnen Instanzen sind untereinander ausfallsicher, sie bieten korrekt gehostet einen maximalen Datenschutz und eine große Unabhängigkeit gegenüber Anbieterentscheidungen.

Wie kam es zum Status Quo?

Wenn viele Argumente also gegen die derzeit in Schulen verwendeten technischen Angeboten sprechen, stellt sich die Frage, wie es überhaupt zu deren Einsatz kam. Die Gründe für die Einführung bestimmter Technologien sind zumeist anhand der Bildungslandschaft und seiner dort vorhandenen wie auch fehlenden Kompetenzen nachvollziehbar.

Fördertöpfe, nicht-Sachkundige und entkoppelte Entscheidungen

Oft treffen die Schulträger die Technologieentscheidungen, dabei sind sie meistens weder praktizierende Lehrer:innen noch Informatiker:innen. Auch sind sie nicht die datenschutzrechtlich verantwortliche Stelle. Folglich stellen sie ihre Bedürfnisse nach Planbarkeit, rascher Funktionalität und Finanzierbarkeit über den Schutz der Privatsphäre der Betroffenen, also der Lehrenden und Lernenden. Sie sehen in der aktuellen Situation zuerst die vom Bund einmalig bereitgestellten Gelder eines Digitalpakts, der keine Aussagen trifft, wie zeitgemäße Schulen aussehen müssen. Die Länder wiederum bieten bei den zu treffenden Entscheidungen wenig Unterstützung, wenn sie einfach nur die Geldtöpfe aufstocken (zum Beispiel in Baden-Württemberg)[34]. Parallel machen die Länder während der Corona-Pandemie ständig neue Vorgaben in Bezug auf die Öffnung beziehungsweise Schließung von Schulen, was die Schulträger unter Handlungsdruck setzt.

Um das Distanzlernen zu garantieren, werden Schulen oft Lösungen aufgezwungen, die gegebenenfalls gar nicht zu ihren Bedürfnissen passen oder die, wie in Hessen festgestellt, schlicht rechtswidrig sind. Stattdessen braucht es eine nachhaltige Entwicklung jeder einzelnen Schule in Abstimmung mit der dortigen Schulgemeinschaft. Eine Grundschule wird mit einer großen Lernplattform überfordert sein oder diese gar nicht richtig nutzen, während sie für ein Gymnasium angemessen ist.

Vom Verwaltungs-Lock-In zum Schul-Lock-In

Manche Schulen gerieten unverschuldet in einen softwareseitigen Lock-In, weil ihre Stadtverwaltungen schon lange auf Microsoft und dessen Sharepoint setzten. Da die Städte oft Schulträger sind und daher für die Ausstattung ihrer Schulen verantwortlich sind, wird passend dazu die Lernplattform Teams ausgewählt. Das macht aus städtischer Sicht Sinn, da entsprechende Verträge nur noch zu erweitern sind, Kosten kalkulierbar scheinen und ihre zu kleinen IT-Abteilungen es leichter haben, wenn alle mit dem gleichen System arbeiten.

Hier zeigen sich die Folgen eines seit vielen Jahren bestehenden Lock-In-Effekts in den kommunalen Verwaltungen[35]. Kaum einer mag bei den damaligen Entscheidungen vorhergesehen haben, dass sie nachhaltige Auswirkungen auf unser Bildungssystem haben werden, weil sich der Lock-In hier fortsetzt. Schulen müssen nun einmal mehr die Versäumnisse der Politik ausgleichen[36].

Internationale Aktiengesellschaften drängen in die Schulen

Firmen wie Google, Microsoft oder Apple sind internationale Aktiengesellschaften und folgen den ökonomischen Interessen ihrer Aktionär:innen. Dafür werden unter anderem Datensammlungen der Nutzer:innen aufgebaut, weswegen es sich für sie lohnt bereits an junge Menschen heranzutreten und sie von klein auf an ihre Produkte und ihre Art der Datennutzung zu gewöhnen. Google spielt im deutschen Bildungsmarkt zwar bisher keine große Rolle. Da sie aber in den USA ein wichtiger Player im Bildungsbereich sind, kann sich das in Deutschland auch langfristig ändern.

Shoshana Zuboff, Professorin für Wirtschaftswissenschaften, kritisierte das auf Datensammlungen basierende Geschäftsmodell einst treffend als „Tyrannei des Überwachungskapitalismus“[37]. Vor diesem Hintergrund ist schwer nachvollziehbar, dass Politiker:innen es zulassen, dass Lehrkräfte und Schüler:innen für diese Geschäftsinteressen dressiert werden. Zumal zusätzlich Lizenzgebühren erhoben werden und es wegen oben beschriebener Geschäftsmodelle auch formaljuristisch zu Datenschutzverletzungen kommt[38].

Natürlich gehören Geschäftsbeziehungen zwischen Firmen und Schulen zum Alltag, woher sonst sollten beispielsweise die technische Ausstattung oder Möbel stammen. Dabei sollten Schulen jedoch werbefreie Räume bleiben, in denen die besten Lösungen anhand klarer Kriterien eingekauft werden und nicht weil ein Anbieter das beste Marketing besitzt oder eine Komplettlösung bereits in der öffentlichen Verwaltung etabliert wurde. Es sollte beim Ausschreiben öffentlicher Aufträge berücksichtigt werden, dass momentan Firmen, deren Geschäftsmodelle auf dem Sammeln von Nutzer:innendaten basieren, auch noch in unsere Schulen einziehen. So wird ihre Marktmacht auf

Kosten von Schüler:innen noch weiter verfestigt.

Über Jahre vernachlässigt, dann geschasst – freie Software

Viele der durch Schulträger und Bildungspolitik ausgelösten Fehlentwicklungen und Irrfahrten, bei denen Software erst eingesetzt werden muss und dann wieder verboten wird, werden auf den Schultern der ohnehin überlasteten Lehrkräfte ausgetragen. Die oft von Lehrkräften oder Dritten geäußerte Folgerung[39], dass der Datenschutz daran schuld sei, ist jedoch falsch. Der Datenschutz ist ein essenzielles Grundrecht. Wenn dieses mit Einführung von bestimmten Technologien mit Füßen getreten wird, sollte die Kritik korrekterweise an Schulträger und Bildungspolitik adressiert werden.

Zudem wird behauptet, dass die Auswahl der Software und Hardware alternativlos sei und dass Datenschutzverstöße von Firmen wie Microsoft geduldet werden müssten, damit der Unterricht auf Distanz weitergehen kann. Zahlreiche funktionierende Gegenbeispiele[40] beweisen, dass dem nicht so ist. Dabei wird gerne verschwiegen, dass die Entscheider:innen diese scheinbare Vormachtstellung selbst provoziert haben. Denn anstelle immer weiter Lizenzgebühren zu bezahlen, könnte man dieses Geld in Weiterentwicklung und Schulung von freier Software investieren.

Besonders überrascht die Entwicklung der Lernstatt Paderborn[41]. Die bereits 2001 gestartete und ständig weiterentwickelte Lerninfrastruktur für insgesamt 37 Schulen wird von einem breiten Zusammenschluss von Firmen, der Universität Paderborn und der Stadt getragen. Pädagogische und technische Fragen werden durch zusätzliche Arbeitsgruppen begleitet. Die hierfür in den Schulen installierten Server werden von einem lokalen Rechenzentrum administriert, um den Lehrkräften den Rücken freizuhalten. Als es zum Distanzlernen kam, stellte sich heraus, dass die Plattform dafür nicht konzipiert war und es kam zu Ausfällen und Cyber-Angriffen. Anstelle mit dem offensichtlich vorhandenen Know-how eigene Lösungen zu entwickeln und das System entsprechend anzupassen, entschied sich die Lernstatt Paderborn Ende 2020 dazu, Microsoft Teams einzukaufen[42].

Ähnliche Problematiken wie in der Bildung bestehen auch an anderen öffentlichen Stellen. Politiker:innen beklagen sich regelmäßig über die Abhängigkeit in der Verwaltung von Microsoft[43], ohne etwas daran zu ändern. Man begibt sich sogar noch tiefer in den Lock-In: Das einstige Vorzeigeprojekt in München unter Verwendung von Linux (LiMux) wurde nach wenigen Jahren eingestellt[44]. Einer der Gründe war, dass nicht alle von der Verwaltung benötigten Anwendungen für Linux verfügbar waren und zu wenig investiert wurde, um diese auf Linux zu portieren oder neu zu entwickeln.

Ausblick – digitale Souveränität fordern und fördern

Wenn wir uns nicht der Herausforderung stellen und nachhaltige Lösungen finden, verlieren wir perspektivisch jede Chance auf digitale Souveränität – nicht nur in der Bildung. Denn je länger Lock-In-Technologien im Einsatz sind, desto schwerer und teurer wird der Wechsel zu anderen Technologien: Lehrkräfte, die über Jahre hinweg ihre Unterrichtsmaterialien mit Lock-In-Software erstellt haben, fällt der Wechsel verständlicherweise schwer. Und je länger wir Lizenzkosten für proprietäre Software zahlen, desto weiter können deren Hersteller diese optimieren, während gerade dieses Geld für die Weiterentwicklung freier Software fehlt.

Produktschulungen verhindern digitale Mündigkeit

Auch leidet die digitale Mündigkeit[45] von Schüler:innen und Lehrenden, wenn sie nur Software-Pakete ausgewählter Hersteller bedienen können. Schon heute begegnen uns immer wieder Personen, die trotz kurzer Einführung nicht in der Lage sind, mit einer anderen Textverarbeitung zurechtzukommen. Neben Produktwissen muss auch Konzeptwissen vermittelt werden, sodass eine Einarbeitung in neue Umgebungen schnell möglich ist.

Hersteller kann Preisschraube jederzeit anziehen

Je schwerer ein Wechsel fällt, desto mehr Geld kann der Anbieter für sein Produkt fordern – die öffentliche Hand übernimmt diese Kosten zwangsweise. Ähnlich wie in der Politik, wo die Kosten für Microsoft-Lizenzen Jahr für Jahr stark steigen[46], besteht dieses Risiko auch für unsere Bildungslandschaft. Wir sollten uns nicht darauf verlassen, dass die Firmen geringe Gewinne akzeptieren, da sie primär an der Bindung der Nutzer:innen interessiert sind beziehungsweise deren Daten sammeln möchten.

Software-Vielfalt statt Monokultur

Eine Software-Vielfalt und die Möglichkeit Software frei den eigenen Bedürfnissen anzupassen, fördert die digitale Mündigkeit von Schüler:innen und Lehrkräften. Würden Schulen diesen Schritt flächendeckend gehen, müsste nicht jede Schule die hohen Kosten für die Anpassungen zahlen. Die öffentliche Hand würde statt Software-Lizenzen nun die Weiterentwicklung von freier Software finanzieren, weitere Kosten fallen für den Betrieb an. Dies schafft lokale Arbeitsplätze und bringt die Software weltweit voran. Genauso wie die Schulen von den Weiterentwicklungen anderer profitieren werden.

Innerhalb der EU ansässige Firmen zahlen im Gegensatz zu manchen globalen Tech-Giganten Steuern auf ihre Gewinne[47]. Mit entsprechenden Budgets kann freie Software in vielen Bereichen den Vergleich zu proprietärer Software halten. Auch Hardware kann länger eingesetzt werden, weil Sicherheitsupdates länger zur Verfügung gestellt werden.

Es werden weniger oft neue Geräte angeschafft, was aus Umweltaspekten nachhaltiger ist und die damit einhergehenden Menschenrechtsverletzungen beim Abbau von Konfliktmaterialien in Ländern des globalen Südens[48] verringert. Langfristig wäre dieser Weg zukunftssicherer. Außerdem verhindert dezentral betriebene Infrastruktur den flächendeckenden Ausfall[49] von Plattformen[50] oder überregionale Leaks von personenbezogenen Daten[51].

Mit digitaler Mündigkeit zu einer freien Wissensgesellschaft

Schüler:innen, deren Know-How sich nicht nur auf den Umgang mit Microsoft- oder Apple-Geräten beschränkt, sondern die ein grundlegendes Verständnis für Technologie entwickelt haben, sind problemlos in der Lage sich kurzfristig Neues anzueignen. Auch wären die Hürden die Software in Politik und Behörden auf freie umzustellen, deutlich geringer und die für unsere Gesellschaft so wichtige und oft geforderte[52] digitale Souveränität wäre langfristig gesichert. Das bei Lizenzen eingesparte Geld stünde unter anderem für die Weiterentwicklung von freier Software zur Verfügung.

Ziel des Schulsystems müssen mündige Menschen sein, die die digitalen Werkzeuge verstehen und hinterfragen können. Digitale Mündigkeit[53] muss über reines Anwendungswissen oder informatische Grundlagen wie das Programmieren hinausgehen. Schüler:innen sollen keine bloßen Nutzer:innen und Werbekund:innen von Plattformen werden, sondern diejenigen sein, die ihre Maschinen kontrollieren und gestalten. Digitalpolitik darf dabei nicht als technischer Randbereich verstanden werden, sondern muss als Grundpfeiler einer modernen Gesellschaftspolitik behandelt werden. Ohne mündige Bürger, im Analogen wie im Digitalen, ist keine Demokratie möglich.

Vor dem Hintergrund der jahrelangen Fehlentwicklungen ist der Weg zu Lock-In-freier Infrastruktur kein leichter, doch je länger wir warten, desto steiniger und teurer wird er. Im Sinne einer freien Bildung, mündigen Bürgern und einer freien Gesellschaft[54] müssen wir ihn gehen. Schulen wären der beste Startpunkt dafür.

1 https://heise.de/-6006927

2 https://creativecommons.org/licenses/by/3.0/de/

3 https://de.wikipedia.org/wiki/Lock-in-Effekt

4 https://de.wikipedia.org/wiki/Lock-in-Effekt

5 https://dach.smarttech.com/erstellung-eines-medienentwicklungs-plans

6 https://excitingedu.de/interaktive-whiteboards/

7 https://ds.ccc.de/pdfs/ds098.pdf

8 https://www.sueddeutsche.de/bildung/schulen-hamburg-hamburger-schule-gibt-allen-fuenftklaesslern-ipads-dpa.urn-newsml-dpa-com-20090101-200928-99-744065

9 https://www.heise.de/meldung/MINT-freundliche-Schulen-iPad-Klassen-Avatare-und-mehr-Bandbreite-fuer-die-Lehrer-3737050.html

10 https://www.bsb-hamburg.de/index.php?id=423#c6911

11 https://e-government.hannover-stadt.de/lhhsimwebre.nsf/DS/1000-2020

https://e-government.hannover-stadt.de/lhhsimwebre.nsf/DS/2754-2020

12 https://www.heise.de/meldung/Fachkraeftemangel-Oeffentlicher-Hand-droht-laut-Studie-Handlungsunfaehigkeit-4365104.html

13 https://www.jamf.com/de/

14 https://www.gbgseelze.de/unterricht/lernangebot/iuk-schulung/

15 https://netzpolitik.org/2020/mit-linux-rechnern-zur-digitalen-nachhaltigkeit/

16 http://www.voris.niedersachsen.de/jportal/?quelle=jlink&query=Verf+ND+Artikel+6c&psml=bsvorisprod.psml&max=true

17 https://www.greenpeace.de/sites/www.greenpeace.de/files/publications/20171016-greenpeace-guide-greener-electronics-englisch.pdf

18 https://fridaysforfuture.de/forderungen/

19 https://buendnis-freie-bildung.de/2020/07/08/hardware-im-bildungsbereich-unsere-empfehlungen/

20 https://www.golem.de/news/aufbereitete-smartphones-augen-auf-beim-refurbished-kauf-2008-150190.html

21 https://schul-frei.org/

22 https://katharineum.de/aktivitaeten/arbeitsgemeinschaften/computer-ag/

23 https://datenschutz.hessen.de/datenschutz/hochschulen-schulen-und-archive/duldung-des-hbdi-für-die-nutzung-insbesondere-us

24 https://dsgvo-gesetz.de/art-17-dsgvo/

25 https://www.datenschutz-mv.de/static/DS/Dateien/Entschliessungen/Datenschutz/20200922_Ent_digitale_Souveraenitaet.pdf

26 https://www.microsoft.com/mea/education/

27 https://www.teamsoft.de/infowelt/microsoft-onenote-class-notebook/

28 https://itslearning.com/de/

29 https://www.ccc.de/de/updates/2017/cms-forderungen

30 https://www.heise.de/news/Microsoft-Office-365-Die-Gruende-fuer-das-Nein-der-Datenschuetzer-4919847.html

31 https://www.belwue.de/angebot/dienste/moodle.html

32 https://km-bw.de/,Lde/Startseite/Service/2020+06+22+Big+Blue+Button+und+Fortbildungsangebote

33 https://www.steuerzahler.de/fileadmin/user_upload/DÖV_2019_Fälle_BW.pdf

34 https://km-bw.de/,Lde/startseite/Service/2020+06+24+Sofortausstattungsprogramm_+Richtlinien+zur+Verteilung+der+Mittel

35 https://www.heise.de/news/Abhaengigkeit-der-oeffentlichen-Verwaltung-von-Microsoft-Co-ist-gigantisch-5058500.html

36 https://www.heise.de/hintergrund/Schule-digital-Lehrkraefte-mussten-die-Versaeumnisse-der-Politik-ausgleichen-5990185.html

37 https://www.blaetter.de/ausgabe/2018/november/kurzgefasst

38 https://digitalcourage.de/blog/2020/datenschutzverstoesse-im-homeschooling-und-bussgelder

39 https://www.heise.de/forum/heise-online/Kommentare/Hessen-beendet-Schonfrist-fuer-MS-Teams-an-Schulen/forum-470562/comment/

40 https://www.ccc.de/de/updates/2021/lockdown-ohne-lock-in

41 https://www.hni.uni-paderborn.de/koi/projekte/lernstatt-paderborn/

42 https://www.westfalen-blatt.de/OWL/Kreis-Paderborn/Paderborn/4349947-Paderborner-Stadtschulpflegschaft-fordert-Team-Bereitstellung-und-besseres-WLAN-an-allen-Schulen-Distanzunterricht-sollte-vereinheitlicht-werden

43 https://www.spiegel.de/netzwelt/microsoft-bundesministerien-kauften-software-fuer-178-millionen-euro-a-00000000-0002-0001-0000-000175196794

44 https://www.heise.de/hintergrund/Verwaltung-Von-Linux-zurueck-zu-Microsoft-4704106.html

45 https://www.ccc.de/de/updates/2017/cms-forderungen

46 https://www.spiegel.de/netzwelt/microsoft-bundesministerien-kauften-software-fuer-178-millionen-euro-a-00000000-0002-0001-0000-000175196794

47 https://t3n.de/news/steuervermeidung-amazon-apple-1229795/

48 https://de.wikipedia.org/wiki/Globaler_S%C3%BCden

49 https://www.heise.de/news/Microsoft-Teams-und-Xbox-Live-zwei-Stunden-lang-nicht-erreichbar-6004764.html

50 https://www.heise.de/news/Zoom-nach-stundenlangem-Ausfall-wieder-verfuegbar-4877985.html, https://www.rbb24.de/politik/thema/2020/coronavirus/beitraege_neu/2020/12/lernraum-berlin-schulen-plattform-serverprobleme.html

51 https://www.heise.de/meldung/Schul-Cloud-gehackt-4723911.html

52 https://www.spiegel.de/netzwelt/microsoft-bundesministerien-kauften-software-fuer-178-millionen-euro-a-00000000-0002-0001-0000-000175196794

53 https://www.ccc.de/de/cms-forderungen-lang

54 https://www.gnu.org/doc/fsfs3-hardcover.pdf

Riko Pieper, Frank Spaeing

„Datenschutz geht zur Schule" (DSgzS)

Eine Initiative des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Im folgenden Artikel stellen die Autoren die Initiative DSgzS vor, beschreiben, wie üblicherweise Veranstaltungen der Initiative ablaufen, welche Erfahrungen bei der Mitarbeit in der Initiative gemacht wurden und versuchen einen Ausblick darauf, wie sich die Arbeit der Initiative in Zukunft weiter entwickeln wird bzw. wie sich das Thema Vermittlung von Datenschutzthemen und Medienkompetenz in Zukunft darstellen kann.

Die Anfänge – Hintergrund/Entstehung

Nachdem bereits mindestens seit 2007/2008 einzelne Datenschützer[1] des BvD ehrenamtlich in Schulen Datenschutzvorträge gehalten hatten, hat sich diese Idee im Jahr 2009 deutschlandweit als BvD[2]-Initiative „Datenschutz geht zur Schule" (DSgzS) etabliert.

Hintergrund war, dass (wir) Datenschützer hauptberuflich die Kollegen (als interner DSB) bzw. Mitarbeiter der Kunden (als externer DSB) über den Datenschutz informieren und beraten. Dadurch soll sichergestellt werden, dass sich einerseits jedermann im Berufsleben an die datenschutzrechtlichen Vorgaben halten kann und andererseits, dass auch jeder über seine Rechte informiert wird und so erfährt, dass auch Andere sich an diese Vorgaben zu halten haben. Das Problem dabei war, dass man von diesen wichtigen Grundkenntnissen zum Datenschutz erst als Erwachsener bzw. beim Eintritt ins Berufsleben etwas erfahren konnte. In der Schule, die einen ansonsten auf das Leben vorbereitet, war (und ist) dieses Thema in den Lehrplänen weitgehend nicht vorgesehen. Die gelebte Praxis war aber – auch damals schon – so, dass Schüler sehr viel online unterwegs waren und entsprechend ihre persönlichen Daten weit gestreut haben (heute vorwiegend über Handys oder Tablets, damals noch hauptsächlich mit PCs oder Laptops). Beim Eintritt in das Berufsleben, das im Normalfall mit Bewerbungen beginnt, kann es dann oft schon zu spät sein für die Erkenntnisse, die einem von einem Datenschützer vermittelt werden[3]. Als möglicher Ausweg aus diesem Dilemma wurden Datenschutz-Sensibilisierungs-Veranstaltungen für Schüler gesehen. Weil man aber nicht warten sollte, bis die Lehrpläne in allen Bundesländern an diese Realität angepasst sind, wurde vom BvD ein neuer Arbeitskreis (AK Schule) ins Leben gerufen, der sich um die Rahmenbedingungen für die gleichzeitig gegründete Initiative DSgzS kümmerte.

Zu den Rahmenbedingungen gehörte zunächst ein einheitlicher Foliensatz, mit dem die Datenschützer (im Folgenden „Dozenten" genannt) ihre Vorträge an den Schulen halten konnten. Schließlich handelte es sich um eine Initiative des BvD, und es sollte daher sichergestellt sein, dass hier im Rahmen der Möglichkeiten auch ein möglichst einheitliches Niveau geboten wird. Dazu gehörten weitere Regelungen wie eine Qualitätssicherung (z. B. in Form von Fragebögen, die am Ende einer Veranstaltung von den Lehrkräften ausgefüllt werden), einem Code of Conduct (CoC), den jeder Dozent zu unterschreiben hat, die Finanzierung (klar geregelte Abläufe z. B. für die Erstattung von Fahrtkosten sowie ggf. Aufwandentschädigungen oder auch Spendenformulare – dazu später mehr), Flyer, Internetauftritt (www.dsgzs.de) sowie die Organisation über die BvD-Geschäftsstelle z. B. für die Anschreiben an die Dozenten als Reaktion auf Schulanfragen, etc.

Zum Qualitätsmanagement der Initiative gehört auch ein „Mentoren- und Freigabekonzept". Abgesehen von den allerersten Dozenten (den Gründern der Initiative), musste jeder weitere Interessent von einem Mentor abgenommen werden – und das ist bis heute so. Erst nachdem man einmal einen Probevortrag in Anwesenheit eines Mentors gehalten hat und dieser Vortrag für „gut" befunden wurde, darf man sich als „Dozent" der Initiative DSgzS bezeichnen und selbstständig vor Klassen auftreten. Dabei muss man weder als Dozent noch als Mentor Mitglied des BvD sein. Es sollte sich jedoch um engagierte Datenschützer handeln, die bereit und in der Lage sind ehrenamtlich Vorträge an Schulen zu halten und sich an die Regeln der Initiative zu halten. Mentoren sind dabei bundesweit verteilte erfahrene Dozenten der Initiative, die zum Zeitpunkt der Ernennung zum Mentor bereits über 1000 Schüler im Rahmen der Vorträge von DSgzS sensibilisiert haben.

Ein Vorfall, der die Initiative in die Nachrichten brachte

Schon während einer der ersten DSgzS-Veranstaltungen gab es folgenden Vorfall, der die Initiative in die Nach-

richten brachte und somit zur Popularität von DSgzS frühzeitig beitrug:

Am Ende einer DSgzS-Veranstaltung trat eine Schülerin an den Dozenten mit folgender Frage heran: „Bei meinem Laptop blinkt manchmal die LED meiner Webcam, obwohl ich sie nicht benutze". Der Dozent dieser Veranstaltung war nicht nur langjährig erfahrener Datenschützer des BvD, sondern auch gut mit Hardware vertraut und in seiner Rolle als IT-Forensiker auch als Gutachter vor Gericht aktiv gewesen. Er konnte schnell einschätzen, dass hier mit hoher Wahrscheinlichkeit etwas nicht stimmte. In Absprache mit der Schule und den Eltern wurde daraufhin die Polizei eingeschaltet. Es stellte sich heraus, dass die Webcam „ferngesteuert" wurde. Die Polizei konnte den Täter über die IP-Adresse ausfindig machen und auf frischer Tat stellen. Als die Wohnung des Täters von der Polizei aufgebrochen wurde, war er gerade online und hatte viele Mädchen-Kinderzimmer auf seinem Bildschirm. Der Mann wurde wenig später verurteilt, jedoch auf Bewährung, weil er ein Ersttäter war. Dieser Vorfall ging damals durch die Medien und wurde auch in den Hauptnachrichten wiedergegeben. Diese Geschichte wird auch heute noch in den DSgzS-Veranstaltungen vorgetragen, weil sie direkt mit der Initiative verbunden ist, und weil sie zeigt, dass gewisse Gefahren nicht nur theoretisch möglich sein können, sondern dass sie auch real stattfinden.

Neben der Problematik, die mit der Bild- und Tonübertragung ins Internet verbunden sein kann, stellte dieser Vorfall auch ein konkretes Beispiel für die Gefahren dar, die mit schlechten Passwörtern verbunden sein können. Der Hacker konnte die Kinderzimmer nämlich nur deshalb „überwachen", weil er auf den PCs/Laptops der Schülerinnen zuvor einen Trojaner installiert hatte. Dies wiederum ging nur, weil er zuvor das Passwort eines Schülers herausbekommen hatte. Mit diesem Passwort konnte er dann dessen Schulkameradinnen (im Namen des Klassenkameraden) kontaktieren, wobei er den Nachrichten ein Bild beifügte, das in Wirklichkeit ein Trojaner war. Durch Aufrufen des langweiligen Bildes, das die Schülerinnen auch bald löschten und schnell wieder vergaßen, wurde die Software installiert, die der Angreifer für die Fernsteuerung der jeweiligen Kameras brauchte.

Solche Geschichten prägen sich bei den Schülern (und Lehrern) deutlich besser ein als das Vortragen von Gesetzen oder die Bitte um Beachtung von TOM[4]. Die mit diesem Beispiel verbundenen Datenschutzthemen (Umgang mit Webcams, Umgang mit Passwörtern) stellen nach wie vor einen wichtigen Teil einer DSgzS-Veranstaltung dar.

Ein Preis, der die Initiative unterstützte

Bei der Preisverleihung des Wettbewerbs „Deutschland Land der Ideen"[5] ging im Jahr 2011 ein Preis an die Initiative DSgzS. Die eingereichte Idee war, dass wir (DSgzS) an einem Tag etwa 1000 Schüler an einem Ort (Berlin) schulen. Dazu wurden zwei Schulen ausgesucht, auf welche die an diesem Aktionstag teilnehmenden Dozenten, die dafür aus ganz Deutschland angereist waren, verteilt wurden. Die Idee wurde prämiert (die Preisverleihung steht unter der Schirmherrschaft des Bundespräsidenten) und ist somit seit 2011 ein weiteres Aushängeschild der Initiative. Bei dieser „Idee" handelte es sich eigentlich nur um eine einmalige Veranstaltung, die für diesen Preis im Jahr 2011 stattfand. Wir wollten die Idee aber aufrechterhalten und haben neben den vielen Veranstaltungen, bei denen jeweils Schulen individuelle Termine mit Dozenten vereinbaren, auch danach jedes Jahr mindestens einen Aktionstag organisiert, bei dem etwa 1000 Schüler an einem Tag geschult werden sollten. Zum Beispiel nutzen wir dazu den jährlich stattfindenden Safer Internet Day (SID)[6], um möglichst vielen Schülern die Teilnahme an einer DSgzS-Veranstaltung zu ermöglichen. Das geschieht bei diesen Veranstaltungen zwar nicht an einem Ort, sondern auf ganz Deutschland verteilt, aber zu anderen Gelegenheiten finden auch nach wie vor regelmäßig solche Veranstaltungen an einem Ort und an einem Tag mit etwa 1000 Schülern statt, zu denen dann jeweils viele Dozenten der Initiative aus ganz Deutschland anreisen (siehe z. B. Dozententag unter „Stand heute").

Stand heute

Nach inzwischen über zehn Jahren DSgzS ist die Grundidee hinter der Initiative unverändert geblieben und der Bedarf ist nach wie vor vorhanden. Es hat sich aber viel getan:

Es stellte sich schnell heraus, dass es neben den DSgzS-Schulveranstaltungen (für Schüler) auch einen Bedarf für Lehrer- und Elternveranstaltungen gibt. Die eigentlichen Schulveranstaltungen waren von Anfang an als kostenlose und ehrenamtliche Veranstaltungen geplant, und das ist bis heute unverändert geblieben, damit keine Unterschiede zwischen Privatschulen und staatlichen Schulen gemacht werden müssen, bei denen zu erwarten ist, dass es Unterschiede in der Bereitschaft (und auch in den Möglichkeiten) gibt, für einen Datenschutzvortrag etwas zu bezahlen.

Veranstaltungen für Erwachsene, die z. B. für das Lehrerkollegium einer Schule oder für Eltern von Schulkindern im Rahmen eines Elternabends gehalten werden, sollten aber nicht vollkommen kostenlos sein. Für die Erwachsenenvorträge sollte es wenigstens einen kleinen Beitrag geben, den der AK Schule dann auf 150,00 € pro Veranstaltung festgelegt hat, von denen 100,00 € netto für die Dozenten sind. Das ist weit entfernt von den üblichen Stundensätzen eines Datenschützers; dazu später mehr unter „Es ist nicht alles Gold, was glänzt – Unterschied zwischen Theorie und Praxis".

Dem AK Schule war klar, dass auch unter Mitwirkung vieler ehrenamtlicher Datenschützer in der Initiative DSgzS der Mangel in den Lehrplänen nicht dauerhaft behoben werden und dass das Engagement somit nur als Übergang gedacht sein kann – bis zu dem Zeitpunkt, an dem wir (DSgzS) uns wieder zurückziehen können, weil der Datenschutz wie auch die Medienkompetenz fest in den Lehrplänen aller Schultypen und aller Bundesländer verankert ist. Wir wussten nur nicht, wie lange es dauern wird und wie wir dieses Ziel erreichen oder mindestens dessen Erreichung forcieren können. Soviel war klar: Wir brauchten Unterstützung.

Zuerst brauchten wir Mitstreiter, die sich an der Arbeit im Arbeitskreis beteiligten. Das war von Anfang an gegeben. Der AK Schule hat zwar eine gewisse

Fluktuation, aber sechs bis zwölf Mitglieder hatte er immer, und damit lässt sich gut arbeiten. Dann werden selbstverständlich Dozenten gebraucht, die in die Schulen gehen – am besten auf ganz Deutschland verteilt. Die meisten Mitglieder des AK sind auch als Dozenten tätig, was aber nicht annähernd ausreicht. An dieser Stelle waren wir nur bedingt erfolgreich. Es gibt ein großes Süd-/Nord-Gefälle, was die Anzahl[7] der Dozenten betrifft. Wir haben in Norddeutschland daher auch extrem wenige Mentoren, die weitere Dozenten freigeben können. Der Autor[8] war deshalb bereits mehrfach im Norden (bis nach Niebüll – etwa 10 km südlich der dänischen Grenze), um auch Norddeutschland in DSgzS mehr einzubinden, und bei diesen Gelegenheiten wurden auch bereits mehrere Dozenten „freigegeben".

Erforderlich waren aber langfristig weitere Mitstreiter auf einer anderen Ebene. Das waren einerseits Sponsoren, welche die Initiative unterstützen konnten, aber auch z. B. Aufsichtsbehörden, die als Referenz in den jeweiligen Bundesländern Gewicht bei den Schulbehörden und den Schulen selbst hatten. Ein erster wichtiger „Mitstreiter" war der (inzwischen ehemalige) Präsident des BayLDA[9], Herr Thomas Kranig, der auch selbst als Dozent der Initiative DSgzS unterwegs war[10]. Die Zusammenarbeit des BvD mit dem BayLDA (auch unter dem Nachfolger Michael Will) und seit Jahren auch mit dem LfDI BW[11], Herr Dr. Stefan Brink, ist inzwischen sehr intensiv und beschränkt sich nicht nur auf DSgzS. Inzwischen wird die Initiative auch von mehreren weiteren Aufsichtsbehörden immer mehr unterstützt, wobei auch hier ein Süd-/Nord-Gefälle erkennbar war, was sich aber zu ändern beginnt. Beispielsweise ist die Landesbeauftragte für den Datenschutz in Niedersachsen[12], Frau Barbara Thiel, schon seit Jahren in der Jury des DAME-Preises[13] des BvD aktives Mitglied und Mitarbeiter der Behörde haben schon an Aktionstagen zum Safer Internet Day (siehe weiter unten) mitgewirkt. Auch das nördlichste Bundesland ist an einer engen Zusammenarbeit mit DSgzS interessiert. Der jährliche „Dozententag" (auf die Dozententage wird in folgenden Abschnitten noch eingegangen) war für 2020 in Kiel im Anschluss an die vom ULD[14] geplante „Sommerakademie" vorgesehen. Bedingt durch Corona musste Frau Marit Hansen, Leiterin des ULD, den Termin zwar absagen, hat die Einladung aber für 2021 aufrechterhalten und sich auch an dem erstmals virtuell durchgeführten Dozententag 2020 als Vortragende beteiligt. Am 3. Juli 2018 veranstaltete Frau Voßhoff – bis 2019 die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) – gemeinsam mit dem BvD in Berlin eine Dialogkonferenz „Datenschutz für Kinder", an der selbstverständlich auch die Initiative DSgzS beteiligt war. Viel mehr geht seitens des BfDI nicht, denn Bildung ist nicht Bundes-, sondern Ländersache.

Neben der hier beschriebenen sehr wichtigen politischen/inhaltlichen/moralischen Unterstützung brauchte die Initiative auch Sponsoren[15], denn es fielen Kosten an, die langfristig weder der Berufsverband (dessen Mitglieder ja nicht unbedingt in DSgzS eingebunden waren) übernehmen konnte und schon gar nicht die ehrenamtlichen Mitglieder der Initiative. Zunächst handelte es sich um geringe Beträge, z. B. für Flyer und weiteres Informationsmaterial, und zunehmend wuchs auch der Arbeitsanteil der Geschäftsstelle für die organisatorische Arbeit. Sponsoren meldeten sich allmählich auch, denn DSgzS ist eine Initiative, an deren Unterstützung Unternehmen aus guten Gründen Interesse haben. Hierzu wurden zunächst ein Flyer[16] und dann ein detailliertes Sponsorenkonzept erstellt. Das Sponsorenkonzept sah unterschiedliche Möglichkeiten der Unterstützung von DSgzS vor. Das reichte von einer rein finanziellen Unterstützung bis hin zu der Möglichkeit, dass Unternehmen z. B. ihre Datenschutzbeauftragten für ein paar DSgzS-Veranstaltungen pro Jahr (jeweils im lokalen Umfeld – um Reisekosten möglichst niedrig zu halten) zur Verfügung stellen konnten.

Seit der Initiative seit einigen Jahren jährlich ein guter fünfstelliger Betrag zur Verfügung steht, gibt es ganz andere Möglichkeiten als in der Anfangszeit. Neben der anteiligen Finanzierung einer Bürokraft in der BvD-Geschäftsstelle, die sich inzwischen hauptsächlich um die vielen organisatorischen Aufgaben der Initiative kümmert, konnten z. B. folgende Ideen umgesetzt werden, an die anfangs gar nicht zu denken war:

- Eine der ersten Ideen war eine konkrete Handreichung zur Unterstützung gegen unbeabsichtigte Nutzung der Webcam (siehe oben: „Ein Vorfall, der die Initiative in die Nachrichten brachte"). Anfangs antworteten die Dozenten auf die Frage, wie man sich davor schützen kann, noch mit dem Hinweis, dass man die Webcam doch abdecken kann, z. B. mit einem Post-it, so lange bis sie bewusst genutzt wird. Jetzt – mit einem nennenswerten Budget – konnten professionellere Lösungen umgesetzt werden. Es wurden u.a. folgende Webcam-Sticker entworfen:



Von den aufgedruckten Symbolen können die folgenden drei als Sticker genutzt werden:





- Damit stehen unterschiedlich große Sticker zur Verfügung, mit denen man entweder die Handy-Kamera oder die Kamera eines Laptops bzw. Monitors oder auch eine externe Webcam abdecken kann. Diese einfachen Webcam-Sticker waren von Anfang an ein großer Renner. Sie werden am Ende jeder DSgzS-Veranstaltung an alle Teilnehmer verteilt. Oft werden weitere Sticker für nicht anwesende Geschwister bzw. die eigenen Kinder der Lehrer nachgefragt[17].
- Eine weitere Handreichung bestand von Anfang an darin, dass „etwas" für die Nachbearbeitung/Vertiefung der DSgzS-Veranstaltungen zur Verfügung gestellt wurde. Engagierte Lehrer haben immer wieder danach gefragt, wie die in den 90 Minuten einer DSgzS-Veranstaltung angesprochenen Themen im Unterricht ver-

tieft werden könnten. Dieses „etwas" bestand anfangs aus Linklisten[18], auf denen zu einem Großteil auf weiterführende Informationen (z.B. auch) von „Klicksafe"[19] verwiesen wurde.

- Mit dem Budget bestand nun die Möglichkeit direkt Handreichungen von Klicksafe speziell für die DSgzS-Veranstaltungen bereitzustellen.
  Die verschiedensten Materialien von Klicksafe können zwar kostenlos von deren Webseite heruntergeladen bzw. in gedruckter Form bestellt werden, aber in dem Umfang, wie es für die DSgzS-Veranstaltungen gebraucht wird, musste dafür eine andere Lösung gefunden werden, damit nicht bei jeder Veranstaltung ca. zehn bis 15 Broschüren und Flyer an die Lehrkräfte übergeben werden mussten.
  Herausgekommen ist eine sehr gute Zusammenarbeit zwischen Klicksafe und DSgzS, deren Endergebnis ein „Lehrerhandout"[20] ist, welches sowohl als PDF-Datei direkt von der DSgzS-Seite (wie auch von der Klicksafe-Webseite) geladen werden kann als auch bei jeder DSgzS-Veranstaltung als gedrucktes Buch kostenlos überreicht wird.
  Inhaltlich handelt es sich dabei um eine speziell auf die DSgzS-Veranstaltungen angepasste Auswahl der Klicksafe-Materialien, bei denen die einzelnen Datenschutzthemen vertieft erläutert und teilweise durch konkrete, im weiteren Unterricht nutzbare Arbeitsblätter ergänzt werden. Die Nachfrage nach diesen Handouts war vom ersten Exemplar an überwältigend. Einige interessierte Behörden (z.B. Landesmedienanstalten) haben diese Handouts beim BvD in großer Stückzahl angefragt – und danach auch noch nachbestellt.
- Als Anerkennung für die ehrenamtlich tätigen Dozenten der Initiative wurde schon lange darüber nachgedacht, wie man den Dozenten für ihr Engagement danken kann, womit sowohl zeitliches als auch finanzielles Engagement gemeint ist; denn manchmal fallen auch höhere Reisekosten an, die nur teilweise an die anfragenden Schulen/Institutionen weitergegeben werden. Als Ergebnis dieser Überlegungen wurde ein jährlicher Dozententag ins Leben gerufen, zu dem alle aktiven Dozenten eingeladen werden. Bisher wurde dazu jedes Jahr ein anderer Ort gewählt (quer über die Republik verteilt, so dass alle ähnliche Reiseaufwände haben), zu dem die Dozenten für eine (mindestens) eintägige Veranstaltung mit vielen interessanten Vorträgen eingeladen werden. Diese Dozententage haben bereits stattgefunden:

  - 2014 an der Ludwig-Maximilians-Universität (LMU) in München
  - 2015 bei der DFS Deutsche Flugsicherung GmbH in Langen (bei Frankfurt)
  - 2016 bei der DATEV in Nürnberg
  - 2017 bei der Deutschen Bahn (DB) in Potsdam
  - 2018 beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) in Stuttgart
  - 2019 im Heinz-Nixdorf-Museum (HNF) in Paderborn
  - 2020 geplant beim ULD in Kiel, online durchgeführt (Corona)
  - dafür 2021 wieder beim ULD in Kiel geplant, muss aber auch online durchgeführt werden[21]

  Den Dozenten werden nicht nur interessante Vorträge rund um die Themen Schule, Bildung, Datenschutz etc. geboten, sondern meistens auch angrenzende Themen, von denen vermutet wird, dass sie für diesen Kreis ebenfalls von Interesse sind: Zum Beispiel wurde 2014 die V2C-Demo (das „Holodeck") vorgestellt, zum Dozententag 2015 waren es VR- und 3D-Brillen einschließlich der dazugehörigen Anwendungssoftware. Außerdem sind auch immer Führungen beim Gastgeber selbst oder in der jeweiligen Umgebung vorgesehen. Beispielsweise gab es bei der Flugsicherung eine Besichtigung des Center Langen, von dem aus der deutsche Luftraum von Düsseldorf im Norden bis zum Bodensee im Süden bis zu einer Höhe von etwa 8000m kontrolliert wird, und in Paderborn konnten die Dozenten das Heinz-Nixdorf-Museum besuchen. In Potsdam fand der Dozententag Dank der Zusammenarbeit mit der Deutschen Bahn im Kaiserbahnhof statt, durch den es natürlich auch eine Führung gab. In Nürnberg wurden vom Gastgeber DATEV Karten für die parallel stattfindende it-sa zur Verfügung gestellt und die Dozenten konnten am frühen Abend einen Vortrag über IT-Forensik im Museum für Kommunikation Nürnberg besuchen. Und in Stuttgart wurde eine Führung über die Baustelle des Hauptbahnhofs (S21erleben) angeboten.
  Bisher haben alle Vortragenden ihre Referate für diesen guten Zweck auch kostenlos gehalten. Hierfür engagierten sich insbesondere Vertreter verschiedener Datenschutz-Aufsichtsbehörden, aber auch z. B. ein Dozent von der Hochschule der Polizei in Thüringen sowie Vertreter von Klicksafe und Verbraucherschutzorganisationen und Andere.
  Abgerundet werden diese Dozententage mit einem gemeinsamen Abendessen am Vorabend und häufig auch mit einem zusätzlichen (vorher stattfindenden) Aktionstag – da ja sowieso viele Dozenten an einem Ort sind. Alle dafür anfallenden Kosten wie das Abendessen und die Hotelübernachtungen sowie die ggf. weiteren Kosten für Catering etc. werden vom BvD – jeweils in Absprache mit den Sponsoren – übernommen.
- Einen Nachteil hatte der ursprüngliche Umgang mit den Spenden jedoch: Der BvD als Berufsverband ist eine Interessenvertretung der Datenschutzbeauftragten und somit im Gegensatz z. B. zur DVD nicht gemeinnützig. Das bedeutet, dass die Spenden versteuert werden mussten, obwohl die Initiative DSgzS ja ehrenamtlich agiert – und somit im Grundsatz sehr wohl gemeinnützig tätig ist. Um das auch rechtlich korrekt darzustellen und somit die Spenden zu 100% auch den vorgesehenen Zwecken zukommen lassen zu können, hatte der BvD-Vorstand im Jahr 2019 die Idee, eine gemeinnützige GmbH zu gründen, was dann auch in einer Mitgliederversammlung so beschlossen und im Jahr 2020 mit Schaffung der BvD-eigenen „privacy4people – Gesellschaft zur Förderung des Datenschutzes gGmbH"[22] umgesetzt wurde. Über diese gGmbH können die Sponsoren jetzt die vollen Spendenbeträge steuerlich absetzen, sofern die

Spenden für die Zwecke[23] der gGmbH vorgesehen sind. Das wird die Spendenbereitschaft sicher zusätzlich erhöhen.

Wie sieht eine DSgzS-Veranstaltung inhaltlich aus – welche Themen werden wie adressiert

Es gibt je nach Alter der Schulkinder zwei unterschiedliche Foliensätze (Sek I und Sek II) – einen für die 5. bis 9. Klassen und einen für die 9. bis 13. Klassen. Bei den neunten Klassen können somit beide Foliensätze genommen werden, was z. B. davon abhängt, ob die Veranstaltungen ansonsten mit 8. Klassen oder mit 10. Klassen gemischt werden.

Die Unterschiede zwischen den Foliensätzen bestehen hauptsächlich in der Einleitung, die für Sek II mehr datenschutzrechtliche Hintergrundinformationen (Historie, DSGVO, BDSG, ...) enthält, während die Einleitung der Sek-I-Vorträge den Datenschutz ausführlicher, anhand von vielen Beispielen auch kindgerechter erläutert.

Nach der Einleitung, die üblicherweise etwa 30 der insgesamt 90 Minuten benötigt, kommt eine Hauptfolie, die sehr viele Themen enthält, aus denen dann individuell Themen ausgewählt werden können. Diese Themenauswahl unterscheidet sich gering in den beiden Foliensätzen; z. B. steht für Sek I folgende Auswahl zur Verfügung (siehe Bild).

Da man für eine DSgzS-Veranstaltung eine Doppelstunde zur Verfügung hat, d.h. 90 Minuten[24], reicht das im Normalfall nicht für alle angegebenen Themen aus. Daher muss eine Auswahl an zu besprechenden Themen vorgenommen werden, was z.B. derart erfolgen kann, dass man abwechselnd den Dozenten und dann die Schulklasse ein Thema auswählen lässt. Wenn ein Thema gewählt wird, dann wird auf weitere Folien (ggf. mit zusätzlichen kurzen Filmbeiträgen) zu dem jeweiligen Thema verzweigt. Am Ende jedes dieser Themen geht es für die nächste Auswahl wieder zur Übersichtsfolie zurück. Bei der Auswahl wird der Dozent immer versuchen, auch die rot dargestellten Themen zu behandeln, weil es sich dabei aus Sicht des AK Schule (der die Folien erstellt hat) um fundamentale Grundlagen handelt, die immer vermittelt werden sollten.

Anhand des Themas „Soziale Netzwerke“ soll beispielhaft erläutert werden, was bei der Auswahl im Detail besprochen und mit den Schülern diskutiert wird; denn was für das Internet allgemein gilt, gilt für die sozialen Netzwerke im Besonderen (siehe speziell den letzten Absatz bzgl. „bewusste Nutzung“). Hier wird anhand von Facebook[25] erläutert, wie diese Plattformen im Grundsatz funktionieren:

In den meisten Fällen bezahlt man keinen Cent für eine Mitgliedschaft, obwohl den Anbietern hohe Kosten entstehen (nämlich z. B. Rechenzeit – und somit Energiekosten, die zur Verfügung gestellte Hardware, die Programmierer und das übrige Personal zur Aufrechterhaltung des Dienstes, usw.), und trotzdem ist es für die Anbieter kein Zusatzgeschäft, sondern sie werden regelrecht reich dabei. Anhand des Beispiels von Facebook wird verdeutlicht, dass alles, was man an Information hinterlässt (und sei es nur ein „Gefällt mir“-Klick) auch etwas wert ist. Die Annahme, dass die eigenen „Banalitäten“, die man von sich gibt, ruhig jedermann lesen kann, und dass sie sowieso niemanden interessieren (außer die eigenen Freunde, für die man es schreibt), ist somit eindeutig falsch. Hiermit wird deutlich gemacht: Man bietet damit als Gegenleistung nichts anderes als eben diese Daten. Sie sind nachweislich in der Summe viele Milliarden Dollar wert! Auf Nachfrage, woher denn das Geld kommt, antworten viele Schüler denn auch prompt: „Werbung“. Diese zweisilbige Antwort wird dann aber vom Dozenten noch etwas erläutert.

Mit den älteren Schülern wird abschließend gern noch folgender Vergleich diskutiert, der auch in den Notizen der entsprechenden Power-Point-Folie allen Dozenten zur Verfügung gestellt wird:

„Wenn man das Verhältnis eines Bauern, der auf dem Markt sein Gemüse verkauft, mit Facebook, dessen Mitgliedern und der Werbeindustrie vergleicht, dann hat Facebook die Rolle des Bauern, die Werbeindustrie die Rolle des (zahlenden) Kunden und man selbst (als Facebook-Mitglied) die Rolle des Gemüses. Viele glauben, dass sie Kunden wären, was aber absolut nicht der Fall ist. Das bedeutet nicht automatisch, dass man deshalb schlecht behandelt wird, so wie auch ein Bauer sein Gemüse hegt und pflegt, aber er macht es, um es zu ernten und Geld damit zu verdienen.“[26]



Ablauf einer Veranstaltung

Wenn eine Schule einen Dozenten der Initiative DSgzS bereits kennt, zum Beispiel weil er in den vergangenen Jahren schon die Vorträge an der Schule gehalten hat, dann kann sie sich direkt an ihn wenden. In solchen Fällen informiert der Dozent dann die AK-Schule-Assis-

tenz, über die alle DSgzS-Veranstaltungen organisiert werden. Die Information darüber, dass es diese Initiative gibt und wo man Bedarf für eine DSgzS-Veranstaltung anmelden kann, kann aus unterschiedlichsten Quellen kommen: Einerseits kann sie aus den vielen Publikationen hierzu vom BvD z. B. in den BvD-News kommen oder auch über die spezielle DSgzS-Seite (dsgzs.de) oder über andere Medien, die von der Initiative berichten (z. B. Klicksafe, oder auch die Nachrichtensendungen von ARD oder ZDF – siehe das oben erwähnte Beispiel „Ein Vorfall, der die Initiative in die Nachrichten brachte"). Andererseits kann es aber auch sein, dass das DSgzS-Angebot sich von Schule zu Schule herumspricht, denn manchmal gehen Geschwister in unterschiedliche Schulen und Eltern aus einer Schule schlagen eine DSgzS-Veranstaltung dann an einer anderen Schule vor.

Sofern eine Schule einen Dozenten sucht, geht die Anfrage über die AK-Schule-Assistenz, und dort wird üblicherweise ein Dozent, der seinen Wohnsitz oder sein Arbeitsumfeld in der Nähe der Schule hat, direkt gefragt. Falls es keinen in der Nähe gibt oder dieser aus anderen Gründen den Termin nicht wahrnehmen kann, informiert die AK-Schule-Assistenz alle abgenommenen Dozenten der Initiative. In den allermeisten Fällen findet sich jemand, der den Termin übernehmen kann. In seltenen Fällen kann es auch vorkommen, dass eine Anfrage nicht zufriedenstellend beantwortet werden kann.

Nachdem der Kontakt zwischen dem Dozenten und der Schule zustande gekommen ist, werden weitere Planungsdetails besprochen. Dazu gehören die jeweiligen Voraussetzungen wie z. B.: Die Schule stellt einen Klassenraum mit Beamer und Leinwand zur Verfügung, und der Dozent bringt einen Laptop mit der erforderlichen Software, den digitalen Vortragsfolien sowie ggf. einen Lautsprecher für die Filme mit.

Außerdem müssen weitere Rahmenbedingungen besprochen werden wie:

- Parkmöglichkeiten für den Dozenten – z. B. auf dem Lehrerparkplatz?
- Treffpunkt mit dem Lehrer/Ansprechpartner der Schule – z. B. Lehrerzimmer.
- Länge einer Veranstaltung: jeweils etwa 90 Minuten (möglichst am Stück – ohne Pause).
- Es muss bei jeder DSgzS-Veranstaltung mindestens ein Lehrer der Schule die volle Zeit mit anwesend sein.
- Am Ende einer DSgzS-Veranstaltung soll ein Fragebogen ausgefüllt werden, der einerseits für die BvD-interne Statistik die Anzahl und die Jahrgangsstufe der Schüler enthält, der andererseits den Lehrern aber auch die Möglichkeit gibt, ein Feedback für die Veranstaltung selbst zu geben.
- Sofern eine längere Anreise erforderlich ist, muss ggf. mit der Schule die Übernahme der Fahrtkosten – oder in seltenen Fällen auch die Übernahme der Übernachtungskosten besprochen werden. Das ist keine Pflicht, aber wenn ein Dozent hier etwas erstattet haben möchte, muss das vorher mit der Schule abgeklärt werden.
- Unabhängig von den Fahrtkosten fällt für Lehrer- und Elternveranstaltungen seitens des BvD eine Pauschale von 150,00 € an, von denen 100,00 € (netto) an den Dozenten weitergegeben werden.
- Falls mehrere DSgzS-Veranstaltungen an einem Tag stattfinden (das ist sogar der Normalfall, damit sich die Anreise lohnt – und außerdem sollen häufig alle Klassen eines oder mehrerer Jahrgänge geschult werden), dann ist es wichtig, dass alle beteiligten Lehrer und Schüler rechtzeitig darüber informiert werden. Dazu mehr unter „Es ist nicht alles Gold, was glänzt – Unterschied zwischen Theorie und Praxis".
- Sofern der Dozent einer der Mentoren der Initiative ist und weitere interessierte Dozenten zum Zuhören oder zum „Abnehmen" eines eigenen Vortrags mitbringen möchte, ist auch das mit der Schule zuvor abzustimmen.

Die eigentliche Durchführung einer DSgzS-Veranstaltung verläuft dann nach einer kurzen Vorstellung – meistens gibt es ein paar einleitende Worte seitens des Lehrers, bevor dieser dann an den Dozenten übergibt – über die digitale Präsentation. Das soll aber nicht heißen, dass die Schüler die gesamten 90 Minuten nur zuhören müssen, denn das wäre sehr anstrengend, bis langweilig. Es wird immer versucht, die Schüler durch Fragen des Dozenten mit in die jeweiligen Themen aktiv einzubinden. Außerdem gibt es zur Auflockerung (und Information) auch viele kurze Filmbeiträge, über die dann anschließend gern und manchmal auch viel diskutiert wird. Oft wird (z. B. in den abschließend auszufüllenden Fragebögen) vorgeschlagen, dass man vielseitigere Unterrichtsmethoden (z. B. Gruppenarbeiten) mit vorsehen sollte. Das geht jedoch aufgrund der kurzen Zeit nicht. Es ist ein Unterschied zwischen dem Vorgehen eines Referendars, der genau solche unterschiedlichen Unterrichtsmethoden lernen und einsetzen soll – und deswegen nach einer Unterrichtsstunde von einem Lehrer beurteilt wird – und dem Stil eines externen Dozenten, der in möglichst kurzer Zeit möglichst viel von seinem Thema vermitteln soll. Speziell junge Lehrer bzw. Referendare, die aktuell noch in der Ausbildung sind, verwechseln das gern mal und setzen die Maßstäbe im Beurteilungsbogen an, die sie aus ihrer Ausbildung selbst erfahren haben. Der AK Schule hat sich diesbezüglich auch mit Medienpädagogen auseinandergesetzt, die bestätigt haben, dass so etwas wie eine Gruppenarbeit in einer DSgzS-Veranstaltung aus Zeitgründen unangebracht wäre. Im Grundsatz ist aber die Art des Vortrags den Dozenten freigestellt. Falls sich also ein Dozent im Einzelfall mal auf eine Gruppenarbeit einlässt, dann ist das auch in Ordnung, solange er dabei nur das Große und Ganze einer DSgzS-Veranstaltung nicht aus dem Blick verliert.

Nach der Einführung in den Datenschutz und den Themen der Übersichtsfolie, die wie beschrieben kaum vollständig besprochen werden können, kommen ein paar Schlussfolien mit weiteren Tipps. Am Ende werden die Webcam-Sticker verteilt, und ein Lehrer bekommt das „Lehrerhandout" ausgehändigt. Im Anschluss wird oft – nach dem offiziellen Ende der Veranstaltung und somit meist in der Pause des Dozenten – noch mit einigen Schülern das eine oder andere persönlich vorgetragene Problem besprochen, das so vor der Klasse nicht diskutiert werden sollte. Auch die Lehrer wenden sich gern noch mit ein paar eigenen Worten (oder auch Problemen)

an die Dozenten, bevor sie sich dann verabschieden, und nicht selten auch, um schon eine weitere Veranstaltung für das Folgejahr zu vereinbaren.

Es ist nicht alles Gold, was glänzt – Unterschied zwischen Theorie und Praxis

In der Theorie würde man erwarten, dass einem Angebot wie den DSgzS-Veranstaltungen von den Schulen, die diese buchen, mit der entsprechenden Aufmerksamkeit begegnet wird.

Um es vorweg zu nehmen: Die meisten Schulen bzw. deren Ansprechpartner (oft die Schulleitung oder ein engagierter Lehrer aus dem Bereich der Informatik oder einem anderen Fachgebiet mit Bezug zur Medienkompetenz) wissen das Engagement der Datenschützer auch zu würdigen und geben sich entsprechend Mühe, dass alles wie zuvor vereinbart funktioniert. Auch die Schüler bedanken sich in aller Regel ausdrücklich am Ende eines Vortrages und nutzen gern die Gelegenheit weitere Fragen zu stellen. Teilweise werden die einleitenden oder abschließenden Worte auch vom Direktor oder dessen Stellvertreter gesprochen, um der Veranstaltung zusätzliche Bedeutung zu verleihen, und manchmal[27] wird zusätzlich der Rundfunk, die Presse oder auch das Fernsehen zu einer DSgzS-Veranstaltung eingeladen.

Es ist auch keine Selbstverständlichkeit, dass Fachleute – egal welcher Zunft – ihren Job in Schulen ehrenamtlich ausführen, für den sie ansonsten ordentlich entlohnt werden. Man kann davon ausgehen, dass es vorwiegend erfahrende Datenschützer sind, die sich an dieser Initiative beteiligen, ohne bei diesem Anlass zusätzliches Geld zu verdienen. Eventuell wird dieses Engagement der Dozenten in den Schulen nicht immer vollumfänglich wahrgenommen. Und möglicherweise wird dieses „umsonst" zur Verfügung gestellte Angebot dahin gehend von manchen falsch verstanden, dass so etwas (Billiges) auch nicht viel wert sein kann und entsprechend wenig Rücksicht/Aufmerksamkeit erfährt.

Der Unterschied zwischen Theorie und Praxis ist tatsächlich in der Praxis oft größer als in der Theorie.

Hierzu ein paar Beispiele:

- Eine regelmäßig wiederkehrende Diskussion kommt zum Thema „Pause" auf. Vereinbart wird immer, dass es sich um eine 90-Minuten-Veranstaltung ohne Pause handelt, denn eine noch so kurze Pause bringt sehr viel Unruhe und ist nie nach der vorgesehenen Zeit zu Ende. Immer gibt es Nachzügler, die erst später wieder in den Raum kommen, was dann jedes Mal erneut ablenkt. Es ist klar, dass 90 Minuten auf die Dauer speziell für die jüngeren Schüler sehr lang sind, aber eine DSgzS-Veranstaltung hört jeder Schüler nur einmal. Bei den Veranstaltungen, bei denen 90 Minuten wie vereinbart durchgeführt werden, funktioniert das gut. Die Schüler brechen nicht zusammen. Die DSgzS-Veranstaltung ist schließlich kein normaler Unterricht, sondern ein „Event" für die Schüler. Es werden keine Hausaufgaben aufgegeben, und es wird danach (seitens der DSgzS-Dozenten) auch keine Arbeit darüber geschrieben. Jeder kann also entspannt zuhören, und wenn er will, kann er sich auch beteiligen – oder auch nicht und dann nur zuhören.
  Dieser und manche der folgenden Punkte haben oft damit zu tun, dass die betreuenden Lehrer manchmal nicht diejenigen sind, mit denen die Absprachen zuvor getroffen wurden. Sie sind nicht die Organisatoren der Veranstaltung, teilweise nur halbherzig dabei und haben ein Problem damit, wenn es eine Abweichung von dem üblichen Unterrichts-Prozedere gibt.
- Es sollte schon aus rechtlichen Gründen[27] eine Selbstverständlichkeit sein, dass bei jeder DSgzS-Veranstaltung auch ein Lehrer der Schule dabei ist, und so wird es auch immer zuvor vereinbart. Falls für eine DSgzS-Veranstaltung mehrere Klassen zusammengelegt werden, stehen auch mehrere Lehrer zur Verfügung. In solchen Fällen fängt manchmal zu Beginn der Veranstaltung die Diskussion darüber an, wer dabeibleiben „muss" und wer jetzt eine Freistunde hat. Wenn es nur eine Klasse ist, dann gibt es diese Diskussion nicht, aber auch in solchen Fällen kam es schon vor, dass der Lehrer von einer Freistunde (für sich) ausging. In manchen Fällen ist der Unmut über die nun doch nicht zur Verfügung stehende Freistunde so groß, dass der Lehrer zunächst fluchend den Raum verlässt – um dann anschließend widerwillig (vermutlich nach Rücksprache mit dem Sekretariat oder der Schulleitung) zurück zu kommen und sich dazu zu setzen. Falls ein Lehrer zu Beginn der Stunde beim Dozenten nachfragt, ob er anwesend sein muss, wird dies jedenfalls klar mit „ja" beantwortet, sofern er der einzige anwesende Lehrer ist.
- Ein ähnliches Thema ist die Pünktlichkeit, mit der die Stunden begonnen werden. Die Dozenten kommen immer mindestens 30 Minuten vor Beginn der Veranstaltung, um in Ruhe aufbauen und alles (Laptop-Anschluss an den Beamer, Lautsprecher, ...) testen zu können. Je nach Gepflogenheiten an der Schule kommen die Schüler und manchmal auch die Lehrer regelmäßig mit deutlicher Verspätung an. Manchmal ist das nur ein Versehen, weil die jeweiligen Fachlehrer und auch die Schüler erst kurzfristig von der Abweichung des normalen Stundenplans (und ggf. des anderen Raums) erfahren haben. Manchmal ist es aber an einer Schule auch einfach üblich, dass der Gong zu Beginn einer Stunde nicht wirklich als „Anfang", sondern eher als „wir können jetzt mal langsam das Pausenbrot zu Ende essen[29] und uns dann auf den Weg machen" interpretiert wird. Der eine Autor war einmal im Jahr 2012 für eine ganze Woche (Montag bis Freitag) an einer Schule in Darmstadt, an der an jedem dieser Tage drei DSgzS-Veranstaltungen hintereinander (also pro Tag 6 Schulstunden) mit einer Gesamtzahl von 769 Schülern in den 5 Tagen durchgeführt wurden. In der anschließenden Woche gab es dann noch einen Elternabend mit 60 Teilnehmern. Folgende Kommentare hatte sich der Autor notiert – und fragt sich heute, warum er das damals nicht abgebrochen hat:
  - Tag 1, 1. Veranstaltung: „Die Veranstaltung hat 15 Min. zu spät angefangen, weil Lehrer/Schüler nicht informiert waren."

- Tag 1, 2. Veranstaltung: „Auch diese 2. Veranstaltung fing gut 10 Min. zu spät an, weil eine der beiden Klassen am Anfang fehlte."
- Tag 1, 3. Veranstaltung: „Auch im 3. Durchgang wurde wieder etwa 5 Min. zu spät angefangen (1. Schultag nach den Ferien.)"
- Tag 2, 1. Veranstaltung: „Eigentlich waren 2 Klassen vorgesehen. Klasse 6a fehlte – keiner wusste warum."
- Tag 2, 2. Veranstaltung: „Diesmal waren beide Klassen am Anfang nicht anwesend. Es wurde mit etwa 15 Min. Verspätung begonnen." Der Dozent erinnert sich, dass er damals nach ein paar Minuten, die er allein im Klassenraum nach dem Gong wartete, ins Sekretariat ging, weil er der Meinung war, dass hier etwas nicht stimmen konnte. Er wurde aber nur verständnislos angesehen und ihm wurde erklärt, dass die Schüler und Lehrer sicher bald kommen würden – was dann ja auch geschah. Verwundert, oder gar peinlich berührt, war jedenfalls niemand.
- Tag 2, 3. Veranstaltung: „Abweichungen vom Plan. Klasse 6a war für morgens geplant. Beginn wurde wieder um gut 10 Min. verzögert."
- Tag 3, 1. Veranstaltung: „Ab hier wurden die üblichen 10 Min. Verspätung als normal betrachtet."

Der andere Autor hat einmal während eines Vortrages an einer Schule in Dessau eine längere Diskussion zwischen dem Vertretungs-Lehrer, der für die Vertretung der Vertretung der ursprünglich geplanten Lehrerkraft im Einsatz war (und dieses wohl auch erst 15 Minuten vorher mitbekommen hatte) und den darum herumsitzenden Schülern verfolgt, die sich zur ständig steigernden Belustigung der meisten Schüler sehr lautstark über die Sinnhaftigkeit und auch die Güte des Vortrages ausließen. Dieses führte zu einem (entgegen der üblichen Gewohnheit des Dozenten) extrem kurzen Vortrag und einem recht abrupten Ende. Einer der Schüler kam zum Ende der Veranstaltung und entschuldigte sich für die Klasse und den Lehrer (keine Selbstverständlichkeit bei 7.-Klässlern).

Aber im Großen und Ganzen sind solche Situationen doch eher die Ausnahme, die Schüler wie auch die Schule und die Lehrkräfte sind dankbar für die und zufrieden mit den Vorträgen und die Dozenten meist nach den Vorträgen zwar geschafft (niemand sollte unterschätzen, wie anders und mitunter auch wie anstrengend Vorträge vor und mit Kindern und Jugendlichen sein können) aber auch mit sich, der Welt und ihrem ehrenamtlichen Engagement im Reinen.

DSgzS in Zeiten von Corona

Dieser Artikel wurde in großen Teilen in den letzten Tagen des Jahres 2020 geschrieben. Der Impfstoff war inzwischen freigegeben, aber eine Mutation des Virus war aufgetaucht, von der man noch nicht viel wusste. Es gab also ein Licht am Ende des Tunnels, aber die Stimmung war trotzdem nur verhalten positiv. Im Jahr 2020 gab es bedingt durch Corona ab März nur noch sehr wenige DSgzS-Veranstaltungen, wie auch bisher im Jahr 2021.

Im Herbst wurde überlegt, ob auch DSgzS-Veranstaltungen online durchgeführt werden könnten. Die Sprecher des AK Schule[30] haben sich mit den Mitgliedern des AK Schule dazu ausgetauscht und diese Frage intensiv diskutiert. Sie waren sich einig, dass sie selbst keine DSgzS-Veranstaltung online durchführen wollen, weil diese Veranstaltungen durch Fragen an die Schüler und die jeweiligen Antworten sehr von der Interaktion leben. Bei der Disziplin, die Online-Meetings beanspruchen, wenn nicht alle durcheinanderreden wollen, ist eine typische DSgzS-Veranstaltung kaum denkbar. Andererseits sollten Online-Veranstaltungen aber auch nicht ausgeschlossen werden.

Es wurde schließlich den einzelnen Dozenten überlassen, selbst zu entscheiden, ob sie die Anfrage einer Schule zu- oder absagen sollten. Im Jahr 2020 wie auch im laufenden Jahr 2021 gab es sowieso nur sehr wenige Anfragen, oft nur mit langem Vorlauf in der Hoffnung, dass sich die Situation bis dahin deutlich entspannt hat, was dann oft zu nachträglichen Absagen seitens der Schulen führte, weil das Virus nach wie vor da war. Es wurde jedoch darauf hingewiesen, dass man im Falle einer Online-Veranstaltung ein paar zusätzliche Punkte prüfen müsste:

- Wer bestimmt das Tool, mit dem die Online-Veranstaltung durchgeführt wird? Der BvD bietet dafür eine Möglichkeit, die auch für DSgzS-Veranstaltungen genutzt werden können. Schulen haben aber evtl. ihr eigenes Tool, das sie auch nutzen wollen (oder evtl. nutzen müssen).
- Funktioniert die Präsentation auch für den Fall, dass ein für den Dozenten neues Tool für das Online-Meeting genutzt wird?
- Funktionieren auch die Filme, die während einer DSgzS-Veranstaltung gezeigt werden, mit dem Tool der Schule?
- Insgesamt muss das alles zu einem Testtermin vor der eigentlichen Veranstaltung ausprobiert werden, damit man während der echten DSgzS-Veranstaltung keine bösen Überraschungen erlebt.

Und so hat es einige Dozenten gegeben, die mal mehr und mal weniger erfolgreich das Online-Format getestet haben. Aber die meisten Aktiven der Initiative sind sich einig, dass sie sich auf die Zeiten freuen, in denen wieder reguläre DSgzS-Veranstaltungen möglich sind.

Vision für die Zukunft

Wie oben unter „Stand heute" bereits angedeutet, entspricht das langfristige Ziel der Initiative und des AK Schule dem der Entwicklungshilfe entliehenen Konzept[31] der „Hilfe zur Selbsthilfe". Gemeint ist damit, dass so ein Projekt irgendwann zu Ende geht und dann trotzdem (also ohne diese Hilfe) allein weiterlaufen soll. Drastischer ausgedrückt: Man hat die Aufgabe, sich überflüssig zu machen[32].

Noch ist dieses Ziel nach inzwischen über 10 Jahren DSgzS nicht erreicht, aber es gibt durchaus Lichtblicke.

Mit Art. 57[33] Abs. 1 lit. b DSGVO ist eine der Aufgaben der DS-Aufsichtsbehörden folgendermaßen beschrieben:

„Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet [...] die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisieren und sie darüber aufklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder;“

Die oben beschriebene gute Zusammenarbeit zwischen den DS-Aufsichtsbehörden und DSgzS ist daher kein Zufall und wird sich sicher noch weiter intensivieren. Es gab auch Aufsichtsbehörden, die schon vor der DSGVO ein entsprechendes eigenes Programm initiiert hatten (z. B. Rheinland-Pfalz), so dass DSgzS-Veranstaltungen in diesen Bundesländern naturgemäß seltener waren. Das hindert aber weder die Aufsichtsbehörden noch die Initiative daran trotzdem gemeinsame Aktionen durchzuführen (z. B. die Aktionstage zum Safer Internet Day – siehe oben).

Neben der Unterstützung durch die Aufsichtsbehörden bei großen Veranstaltungen (wie z. B. zu Dozententagen) gibt es immer mehr Mitarbeiter von Aufsichtsbehörden, die sich aktiv an DSgzS-Schulungen beteiligen (also nicht nur der Chef selbst). Das Konzept zur Freigabe der Dozenten durch die Mentoren der Initiative wurde daher in Bezug auf Mitarbeiter von Aufsichtsbehörden dahingehend gelockert, dass diese nicht explizit freigegeben werden müssen. Das ist in Bezug auf Aufsichtsbehörden auch angemessen, denn eine Freigabe durch einen Mentor der Initiative (der ja meistens auch DSB im Zuständigkeitsbereich der Aufsichtsbehörde ist) hätte langfristig ein „Geschmäckle“. Dass sich der ehemalige Chef des BayLDA dieser Prozedur unterzogen hat, war aber trotzdem eine schöne Geste.

Durch die Corona-Pandemie gab es einen nie dagewesenen Schub in Richtung Homeoffice und in Bezug auf Schulen und Schüler auf „Homeschooling“. Die seit vielen Jahren angekündigte, aber immer wieder vernachlässigte Förderung der „Digitalisierung“ wurde daher in den Jahren 2020/2021 endlich (wenn auch ursprünglich ungeplant) vorangetrieben. Eng damit verbunden ist jedoch der korrekte Umgang mit personenbezogenen Daten, auch wenn für manche der Datenschutz eher als Hemmnis für die Digitalisierung empfunden wird und nicht als deren wesentlicher Bestandteil. Das Feedback der meisten Schüler und Lehrer bestätigt jedoch immer wieder, dass die Beherrschung der Technik zwar eine notwendige, aber keine hinreichende Voraussetzung für den korrekten Umgang untereinander ist.

In diesem Sinne bleibt zu hoffen, dass die Corona-Pandemie den Ruck in die Gesellschaft gebracht hat, den der ehemalige Bundespräsident Roman Herzog in anderem Zusammenhang[34] einmal für Deutschland gefordert hat.

1 Die Verwendung männlicher Sprache erfolgt im Interesse von Klarheit, Kürze und Einfachheit verbunden mit der Bitte, nicht das grammatische Maskulinum auf das biologische Geschlecht zu reduzieren.

2 BvD steht für „Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.“, www.bvdnet.de

3 Gemeint sind hier nicht die technischen, organisatorischen oder rechtlichen Details, sondern hauptsächlich die Grundaussage, dass man vorsichtig sein sollte, wenn man sowohl eigene als auch fremde Daten (im Internet) streut. Man sollte immer im Hinterkopf behalten, dass dies auch andere Personen lesen können als die eigentlichen Adressaten der Veröffentlichung.

4 „TOM“ steht im Datenschutz für „technische und organisatorische Maßnahmen“. Aus den hier genannten Gründen werden diese Themen in einer DSgzS-Veranstaltung nur kurz angerissen. Zur Vertiefung dieser Themen reicht die Zeit einer DSgzS-Veranstaltung nicht aus, aber jeder Schule wird ein (kostenloses) Lehrerhandout überlassen (siehe oben unter „Stand heute“), das von der DSgzS-Seite auch als PDF heruntergeladen werden kann.

5 https://land-der-ideen.de/

6 https://www.klicksafe.de/ueber-klicksafe/safer-internet-day/

7 Die Initiative DSgzS hat in der Liste der Dozenten eine größere Anzahl von „Karteileichen“ – also Dozenten, die zwar anfangs Interesse gezeigt haben und dann auch von einem Mentor als Dozent bestätigt wurden, sich aber danach kaum noch bei Anfragen zu DSgzS-Veranstaltungen gemeldet haben.

8 Gemeint ist hier und im folgenden Text mit „der Autor“ immer mindestens einer der beiden Autoren dieses Artikels.

9 Bayrisches Landesamt für Datenschutzaufsicht (BayLDA) – URL: https://www.lda.bayern.de/

10 Herr Kranig ließ sich dazu, wie jeder andere Dozent auch, von einem Mentor von DSgzS als Dozent „freigeben“.

11 Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg (LFDI BW) – URL: https://www.baden-wuerttemberg.datenschutz.de/

12 https://lfd.niedersachsen.de/startseite/

13 DAME steht für „Datenschutz Medienpreis“ – URL: https://www.bvdnet.de/datenschutzmedienpreis/

14 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein – URL: https://www.datenschutzzentrum.de/

15 Liste der Sponsoren: https://www.bvdnet.de/wp-content/uploads/2016/11/DsgzS_Sponsoren.pdf

16 https://www.bvdnet.de/wp-content/uploads/2016/11/DsgzS_Sponsoren.pdf

17 Unsere Renten sind also wirklich sicher.

18 Linkliste für Schüler: https://www.bvdnet.de/wp-content/uploads/2017/10/linkliste_dsgzs_schueler.pdf, Linkliste für Lehrer/Eltern: https://www.bvdnet.de/wp-content/uploads/2017/10/linkliste_dsgzs_lehrer_eltern.pdf

19 https://www.klicksafe.de/ - Auszug aus dem Impressum: „Die Website www.klicksafe.de ist Bestandteil der Initiative klicksafe im CEF (Connecting Europe Facility) Telecom Programm der Europäischen Union für mehr Sicherheit im Internet. Die EU-Initiative klicksafe ist politisch und wirtschaftlich unabhängig und wird in Deutschland von den Medienanstalten in Rheinland-Pfalz (Koordinator) und in Nordrhein-Westfalen umgesetzt.“

20 https://www.bvdnet.de/datenschutz-geht-zur-schule/lehrerhandout/

21 Auch 2021 muss der Dozententag online stattfinden, da die als Incentive gedachte Sommerakademie des ULD im Jahr 2021 abgesagt wurde. Aber alle gute Dinge sind drei, wir planen es nun für das Jahr 2022, nach Kiel zu gehen.

22 „gGmbH“ steht für „gemeinnützige Gesellschaft mit beschränkter Haftung“ https://www.bvdnet.de/privacy4people-gesellschaft-zur-foerderung-des-datenschutzes-ggmbh/

23 Neben der Initiative DSgzS gehört auch der oben bereits erwähnte „Datenschutz Medienpreis“ (DAME) zu den Zwecken, die von der „privacy4people“ gefördert werden.

24 Eine Schulstunde dauert im Normalfall 45 Minuten, eine Doppelstunde daher

90 Minuten. Manchmal sind noch kurze Pausen von 5 Minuten vorgesehen, die aus Zeitersparnisgründen möglichst nicht genommen werden. Die Unterbrechung wäre in der Praxis deutlich mehr als diese vorgesehenen 5 Minuten, und die Zeit ist sowieso sehr knapp. Meistens gibt es keine Diskussion darüber, aber manchmal muss die Pause auch genommen werden.

25 Am Anfang von DSgzS waren noch viele Schüler bei SchülerCC, SchülerVZ und anderen sozialen Netzwerken, die es heute gar nicht mehr gibt.

26 Nach Redaktionsschluss sind wir noch auf das folgende Interview mit dem BfDI Prof. Kelber gestoßen, dessen Aussage sehr ähnlich ist: Datenschutzbeauftragter im Kinder-Interview - »Ihr seid nicht die Kunden, ihr seid die Ware« www.spiegel.de/deinspiegel/datenschutzbeauftragter-ihr-seid-nicht-die-kunden-ihr-seid-die-ware-a-9356a519-0002-0001-0000-000177426669

27 Speziell zum jährlich stattfindenden Safer Internet Day (SID) gibt es oft viele Aktivitäten an Schulen, zu denen dann teilweise auch die Medien eingeladen werden.

28 Die Schule und somit der jeweils betreuende Lehrer hat eine Aufsichtspflicht. Das gilt nicht für den Dozenten, der nur als Gast an der Schule ist. Falls es einen Vorfall gibt (z.B. könnte einem Schüler schlecht werden oder es könnte ein anderes gesundheitliches Problem auftreten) weiß nur der Lehrer an wen man sich in so einem Fall zu wenden hat bzw. wie damit umzugehen ist.

29 Wobei man sich auch in Erinnerung ruft, dass man beim Essen ja nicht hetzen soll.

30 Es gibt einen Sprecher und zwei Stellvertreter. Die beiden Stellvertreter sind die Autoren dieses Artikels.

31 Der eine Autor war selbst 6 Jahre im Rahmen der Entwicklungshilfe an einem Fischereiforschungsinstitut in Mar del Plata, Argentinien, beschäftigt. Der Informatik-Bereich, den er damals aufgebaut hatte, existiert bis heute.

32 Was man aus Sicht der Autoren auch von jedem guten Berater erwarten sollte.

33 Aufgaben der Aufsichtsbehörden, https://www.datenschutz-wiki.de/DSGVO:Art_57

34 Die Berliner Rede war eine vom damaligen deutschen Bundespräsidenten Roman Herzog am 26. April 1997 in Berlin gehaltene öffentliche Ansprache. Die von Herzog in dieser Rede gewählte Formulierung „durch Deutschland muss ein Ruck gehen" ließ diesen Vortrag als Ruck-Rede in die Geschichte eingehen.

Dr. Joachim Paul

Schule digital: Bildungsmedien für Schulen – bundesweites Kuddelmuddel

Medienplattformen könnten Lernplattformen mit guten Lerninhalten versorgen, allerdings herrscht auch hier viel Chaos. Joachim Paul kommentiert, was fehlt[1].

Die Coronavirus-Pandemie und der damit einhergehende Wechsel zum Distanzlernen haben deutlich gezeigt, dass die bislang von Bund, Ländern und Kommunen aufgebaute digitale Bildungsinfrastruktur in Deutschland bisher nicht in der Lage war die Ausfälle des Präsenzunterrichts entsprechend zu überbrücken. Dass die vollständige Katastrophe ausblieb, ist ein weiteres Mal dem Einsatz von Lehrkräften zu verdanken. Ihnen wird regelmäßig vorgeworfen, sie seien größtenteils Digitalmuffel. Dass sie nun das ausbaden mussten, was Politikerinnen und Politiker in den vergangenen Jahren versäumt haben, ist aber mehr als klar.

Fehlender digitaler Bildungscontent

Unerledigte Hausaufgaben und fehlender politischer Mut sind den Landespolitiken zuzuschreiben, der Kultusministerkonferenz KMK sowie der Bundespolitik. Deren Defizite zeigen sich nicht nur im zu späten oder unzureichenden Ausbau und Betrieb von Lernplattformen, wie verschiedentliche Zusammenbrüche und Überlastungsphänomene von mehreren Plattformen belegen, sie liegen – und das soll hier Thema sein – auch in der Beschaffung und Bereitstellung von qualitätsgeprüftem digitalen Bildungscontent für den Kontext Schule.

Meine These: Es ist alles schon da und das seit Jahren. Das Geld sollte nur an der richtigen Stelle ausgegeben werden. Die bereits vorhandenen Angebote sollten entsprechend gefördert, ausgebaut und auch verknüpft werden. Da dies nicht der Fall ist, führen einige Kritiker gern den Föderalismus als einzig Schuldigen an. Das ist jedoch eine Nebelkerze. Denn Kommunikationsprobleme rangieren hier aus meiner Sicht über den Strukturproblemen. Und wäre eine klare Strategie da, erledigten sich auch Reibungsverluste und die Förderung fruchtloser Doppelstrukturen.

Wo sind die Inhalte?

Beginnen wir von vorne: Sehr lange Zeit wurde die Digitalisierung der Schulen von der Bundespolitik wesentlich mit der Ausstattung mit Hardware, WLAN und Netzanschlüssen gleichgesetzt. Mit Hardware ausgestattet wurde zwar zum Teil, aber auch das nur unzureichend. Erst während der Pandemie, so scheint es, wurde auf Bundesebene zusätzlich bemerkt, dass Bildungsinhalte ebenfalls zählen, dass – ins Analoge übertragen – Klassenzimmer ohne Medienregale oder Schultafeln ohne Kreide einfach nicht sinnvoll sind. Daher wurden hierfür weitere Mittel aus dem Digitalpakt[2] bereitgestellt.

Aber was haben hier die Länder und der Bund im Angebot? Was gibt es bereits und wo setzen Bund und Länder mit der Schaffung weiterer Angebote an?

Versteckte Inhalte und Plattformen

Recht leistungsfähige Plattformen für die Distribution von digitalen Bildungs-

medien speziell für Schulen gibt es in allen 16 Bundesländern, und das teilweise seit mehr als 15 Jahren, bereitgestellt entweder vom jeweiligen Bundesland oder durch Kommunen oder kommunale Kooperationen. Denn für die Beschaffung von Sachmitteln für Schulen – dazu gehören auch die digitalen Medien – sind die Schulträger zuständig, also die Kommunen. Diese kaufen digitalen Content allerdings nur für den eigenen Bereich. Die Nutzungslizenzen der Medien sind daher auf die eigene Kommune oder das eigene Bundesland beschränkt, die Medien sind also keinesfalls bundesweit oder gar frei verfügbar.

Diese Plattformen sind zudem nicht im allgemeinen Bewusstsein und oft leider auch nicht im Blick der Bundespolitik. Sie tauchen selten bis nie in der überregionalen Berichterstattung zu Bildung und Digitalisierung auf. Die Aufmerksamkeit der Medien gehört hier in schöner Regelmäßigkeit dem Nutzen von Youtube in Schulen oder den Mediatheken der großen Sender. Die bundesweiten Aktivitäten der Politik konzentrieren sich zugleich – getragen von der Kultusministerkonferenz der Länder (KMK) sowie vom Bundesministerium für Bildung und Forschung (BMBF) – unkoordiniert auf die Bereitstellung von zwei Suchmaschinen für sogenannte freie Bildungsmaterialien.

Doppelt gemoppelt und bislang ohne Schnittstellen

Blicken wir also zunächst in Richtung Bund. Um Lehrkräften den Zugriff auf digital und frei verfügbares Lehr- und Lernmaterial zu erleichtern, wurden zwei Plattformen im Rahmen des Digitalpakts Schule gegründet. Zum einen „WirLernenOnline“ (kurz WLO), zum anderen „MUNDO“, ein ländergemeinsames Projekt und realisiert vom FWU Institut für Film und Bild in Wissenschaft und Unterricht GmbH, dem Medieninstitut der Länder, im Auftrag der KMK. Was sie bisher leisten ist aber sehr fragwürdig.

Während die Bundesregierung auf „zwei leistungsfähige OER-Suchmöglichkeiten“ verweist, diagnostiziert der Journalist Christian Füller unter dem Titel „Zwei Plattformen sind eine zu viel“[3] im Tagesspiegel folgerichtig eine Konkurrenz um die Aufmerksamkeit der Lehrkräfte und berichtet, dass Frau Ministerin Karliczek vom Bundesministerium für Bildung und Forschung es gut findet, „wenn sich Angebote für das Onlinelernen ergänzen“. Aufmerksamkeit aber – zumal die der Lehrkraft – ist ein knappes Gut.

Was können also diese Plattformen?

Wir lernen online

Wir Lernen Online ist schon seit März 2020 online und ein Produkt einer Konsortialgemeinschaft, bestehend aus dem Verein edu-sharing.net e.V., der Wikimedia und dem Bündnis Freie Bildung im Community-Management. Neben der Suchfunktion gibt es bei WLO auch schulfachspezifische Portale. Die Oberfläche sieht ansprechend aus und vermittelt den Eindruck der leichten Bedienbarkeit, die Funktion „Filter“ allerdings hat es in sich.

Die Suchtreffer zu einem Stichwort können nach Schulfächern, Altersstufen, Medienarten, Bezugsquellen und Schlagworten nachträglich gefiltert werden, wobei nur die Filterkriterien angeboten werden, die in der aktuellen Suchtrefferliste auch tatsächlich vorhanden sind – der Vorteil einer indexbasierten Suche. In vielen Länderportalen ist das allerdings längst Standard. Unter den Bezugsquellen findet sich nicht selten sogar Youtube.

Ein Portal, das Youtube nach Bildungsinhalten durchsucht? Das macht Sinn. Wenn nicht in so einigen Youtubetreffern Werbeeinblendungen wären. In Schulen ist das ein absolutes No-Go. Ließe man das offiziell und mit staatlicher Förderung zu, dann wäre das der Durchschlag der neoliberalen Version der Aufmerksamkeitsökonomie in den Schutzraum Schule. Hier müssen die Portalbetreiber nachbessern. Das ist möglich, denn es ist filterbar, ob ein Youtube-Kanal auf Werbeeinblendungen setzt oder nicht.

Open Educational Resources

Bei WLO wird die OER-Philosophie offensiv vertreten. Für Nicht-Insider: Die Abkürzung OER steht für „Open Educational Resources“. Darunter werden freie Lern- und Lehrmaterialien mit einer offenen Lizenz wie etwa Creative Commons oder GNU General Public License in Anlehnung an den englischen Begriff für Freie Inhalte, open content, verstanden.

Daher gibt es über der Suchworteingabe einen Schiebeschalter, über den die Funktion „zeige mir nur OER“ aktiviert werden kann. Angezeigt werden dann ausschließlich Treffer, deren Medien unter einer Creative Commons Lizenz stehen. Checks mit verschiedenen Stichworten zeigen, dass sich die Anzahl der Suchtreffer für echte OER-Medien im Schnitt auf ein Zehntel bis ein Fünftel reduziert. Das ist enttäuschend, jedoch nicht der Suchmaschine anzulasten. Aber warum das so ist, das muss diskutiert werden.

Hier gibt es nichts zu sehen

Die Eingabe des Stichworts „Vogel“ bei WLO liefert 480 Treffer, auf Platz 6 gar den „Vogel des Jahres 2016“, ein Wissenshappen vom ZDF, präsentiert von Harald Lesch (Stand 17.04.2021). Ein Klick auf den Link führt zur ZDF-Mediathek und dort zu der Meldung „Diese Seite wurde leider nicht gefunden – Der von Ihnen gewünschte Inhalt ist nicht mehr vorhanden“. Das ist eine Folge des gültigen Staatsvertrages, der den Sender anweist, Inhalte nur für eine bestimmte Zeit in der Mediathek vorzuhalten. Nun ist aber die Frage an WLO berechtigt – wenn man schon auf eine indexbasierte Suche statt eine Echtzeitsuche in externen Repositorien setzt – wie oft der Index aktualisiert wird. Fakt ist: Derselbe ins Leere führende Treffer wird im konkreten Fall mehrere Wochen lang angezeigt. Lehrkräfte, die etwas suchen, nehmen solche Leerläufe übel, wenn sie öfter auftreten.

Des weiteren verblüfft die Relevanzsortierung der Treffer. Bei so manchen Stichworten, zum Beispiel „Igel“ oder „Elefant“, fällt es schwer, darin irgendeinen Sinn oder ein System zu entdecken. Außerdem sind die Datensätze zur Beschreibung der Medien, die sogenannten Metadaten, oft nicht sauber.

MUNDO

MUNDO ist ein Teil von SODIX, das als Projekt die von der KMK formulier-

ten Herausforderungen über zentrale, service-orientierte und landesspezifisch anpassbare Lösungen adressiert. Die Kultusministerkonferenz der Länder setzt mit ihrer im Dezember 2016 veröffentlichten Strategie „Bildung in der digitalen Welt“[4] verbindliche Maßstäbe für die Digitalisierung der Bildungssysteme der Länder und benennt in diesem Zusammenhang auch konkret die Anforderungen an eine zu entwickelnde Bildungsmedieninfrastruktur. Dazu gehören 1. die allgemeine Auffindbarkeit von Bildungsmedien, 2. allgemeine und jederzeitige Verfügbarkeit von Bildungsmedien, 3. allgemein verbindliche technische Schnittstellen und 4. öffentliche Dokumentation.

Das heißt: Für MUNDO ist zumindest die Möglichkeit der Integration in Ländersysteme nicht nur in Aussicht gestellt, sie ist obligatorisch, denn sie ist Gegenstand eines Auftrags der KMK.

Die Oberfläche von MUNDO ist vergleichbar mit WLO ansprechend gestaltet und bietet auch vergleichbare Funktionen. Ebenso wie bei WLO gibt es Filter für Schulfächer, Schulstufen, Medienarten und Lizenzarten, die CC-Lizenzen sind hier sogar feiner gerastert. Auch hier wird versucht, die Vorteile einer indexbasierten Suche voll auszuschöpfen. Bei Zuschaltung eines Filters wird unmittelbar die Anzahl der verbleibenden Treffer angezeigt. Allerdings sucht man bei vielen Stichworten vergeblich nach einer sinnvollen Relevanzsortierung, ebenso wie bei WLO. Wie bewerten Lehrkräfte das?

Gute Idee, schlecht umgesetzt?

Am 18. September 2020 – zu diesem Zeitpunkt waren noch nicht alle heute verfügbaren Funktionen realisiert – veröffentlicht der Deutschlandfunk einen Beitrag „Bildungsportal MUNDO im Lehrercheck“[5]. Eine Lehrerin und ein Lehrer aus Berlin, sie für Englisch und Russisch, er für Mathematik, probierten das Portal aus. Ihre Kommentare reichten von „kenne ich schon“ über „das ist wie Youtube“ bis hin zu „das sind nur Links“. Die Lehrerin bemängelte zusätzlich das Fehlen von Aufgabenstellungen und Fragen. Und der Mathematiklehrer ergänzte: „Also ich brauche diese Meta-Ebene nicht. Ich kann mir dieselben Sachen auch ergoogeln.“

MUNDO erneut nutzen würden beide nicht. Das ist vernichtend. Und es darf behauptet werden, dass bei WLO das Urteil ähnlich ausgefallen wäre, denn beide Systeme sind im Wesentlichen Sammlungen von Internetlinks. Die umfangreichen und komfortablen Filterfunktionen beider Systeme können die inhaltliche Armut des Angebots nicht kaschieren, so bleiben sie vielmehr technischer Ausdruck politischer Hilf- und Konzeptlosigkeit. Wo es nicht viel gibt, kann nicht viel gefunden werden.

Die „Meta“-Strategie der Bundesregierung

In der Antwort auf eine Anfrage der FDP (15.09.2020, Drucksache 19/224776)[6] zu freien Bildungsressourcen erwähnt die Bundesregierung – Scherz am Rande: Unter Angabe eines falschen Links – ein weiteres Projekt namens Jointly, über das Kooperationen und Expertenworkshops zu OER-Themen finanziert werden.

Im Bereich OER-IT der Projektwebsite findet sich ein kurzes Video mit verschiedenen Statements der an dem Projekt beteiligten Personen, in dem mehrfach der Wunsch der Schaffung eines zentralen Adressbuches zur Auflistung von Repositorien geäußert wird. Genau das aber wollen WLO und MUNDO ja leisten. Insofern ist die Frage zu stellen, wo denn was schiefläuft oder unzureichend bleibt. Das Engagement und die Ernsthaftigkeit der an Jointly beteiligten Fachmenschen soll ausdrücklich nicht in Zweifel gezogen werden, im Gegenteil. Aber die Frage bleibt, was von den dort erarbeiteten Konzepten denn in die Tat umgesetzt wird, und zwar so, dass es in Schulen auch ankommt. Hier zeigt sich ein weiteres Mal, die Förderung durch die Bundespolitik ist mehr so meta.

OER ist nicht gleich OER

Ein Problem liegt darin, dass versucht wird, unter dem Label OER Vieles über einen Kamm zu scheren. Denn der Begriff bedient sehr unterschiedliche Bereiche. So ist beispielsweise die Produzierendenstruktur in universitären Kontexten eine völlig andere als in schulischen Bezügen. Für Universitäten und Hochschulen gibt es kaum extern Produzierende wie etwa Schulbuchverlage. Der Löwenanteil der Inhalte kommt von den Lehrkräften der Hochschulen. Und von den Studierenden darf durchaus erwartet werden, dass sie über genügend Selbstlernkompetenz verfügen, sich nicht passgenaues außeruniversitäres Material für ihre Lernprozesse selbstständig zunutze zu machen.

Eine Strategie zur Förderung von OER an Hochschulen tut ganz sicher Not und verdient eigene Beiträge, sie passt aber nicht für den schulischen Kontext, denn dort herrschen andere Randbedingungen. So greift die schulische Lehrkraft für die Gestaltung von Lernprozessen in der Regel auf extern produzierte und aufbereitete Bildungsmedien zurück – wie Schulbücher oder anderweitige Medien – und passt diese Inhalte den aktuellen Erfordernissen der Lernprozesse und ihrer Lernendenkreise an. Erst jetzt wird die Lehrkaft auch – in gewissem Sinn – zum Autoren ihrer Unterrichtsstunde, sie beginnt jedoch, was die Medien angeht, so gut wie nie bei Null. Und sie ist angewiesen auf gutes vorgefertigtes Material, auf bildungsmediale Knetmasse.

Kreis- und Landeslizenzen

Ein weiterer Punkt ist: Es gibt qualitiativ hochwertiges digitales Bildungsmaterial, das kommerziell produziert wurde. Man findet es in den bereits erwähnten Distributionsplattformen der Länder und Kommunen. Der bundesweiten Bereitstellung steht allerdings entgegen, dass Kommunen und Länder diese Medien nur für die Schulen im eigenen Bereich lizenzieren, als Kreislizenzen oder Landeslizenzen.

Eine wichtige Frage an die Bundesregierung lautet also: „Was wäre denn notwendig, damit eine Öffnung dieser Landeslizenzen für die Nutzung in Schulen im gesamten Bundesgebiet möglich ist?“ Für einen konkreten Antwortvorschlag muss ein Blick auf den Markt der Bildungsmedien geworfen werden.

Der Markt der Bildungsmedien und die Digitalisierung

Dieser Markt ist durch seine Geschichte und durch die Medienarten und ihre technisch sehr unterschiedlichen Beschaffenheiten – auf der einen Seite

Bücher, auf der anderen Filme und Video – und durch ihre Verfügbarkeiten bestimmt. Er besteht daher für die Nutzung im Kontext Schule und völlig aus der Zeit gefallen aus zwei immer noch stark voneinander getrennten Bereichen: Dem Schulbuchmarkt und dem Markt für digitale Bildungsmedien mit audiovisuellen Inhalten, der aus dem Markt für den klassischen Unterrichtsfilm hervorging.

Die Nutzungsmöglichkeit der Medien im Bildungskontext wird in diesem Marktbereich in Deutschland durch das System der kommunalen und Landesmedienzentren gewährleistet und ist gesetzlich verankert. Stellvertretend und als Beispiele seien hier zwei Bundesländer angeführt. Die Situation in den anderen vierzehn Ländern ist vergleichbar.

Nach §79 des Schulgesetzes des Landes Nordrhein-Westfalen ist die Lehrmittel- und Medienbereitstellung eine Pflichtaufgabe der Schulträger, also der Kommunen, die Verleih- und Onlinebereitstellung ihren Medienzentren übertragen. Der zuständige Paragraph im Schulgesetz des Freistaats Bayern trägt ebenfalls die Nummer 79 und immer noch den Titel „Bildstellenwesen“. Bildstellen, so hießen die Medienzentren früher – sehr viel früher.

Ungleiche Verteilung

Die Größe dieses Bereichs entspricht daher in etwa den summierten Beschaffungsbudgets der Medienzentren im Bundesgebiet und kommt bestenfalls auf eine zweistellige Millionensumme. Dem gegenüber besitzt der bundesdeutsche Schulbuchmarkt ein Gesamtvolumen von etwa 700 Millionen Euro. Bedingt durch die unterschiedlichen Bereichsgrößen in Euro ergibt sich eine stark divergierende Struktur der Unternehmen und Akteure.

Während der Schulbuchmarkt mit insgesamt etwa 80 Verlagen durch ein Oligopol von drei großen Verlagen bestimmt ist, die etwa 90 Prozent des Umsatzes generieren, besteht der Markt der digitalen Bildungsmedien aus ebenfalls etwa 80 jedoch kleineren mittelständischen Unternehmen mit zwei bis 20 Mitarbeitenden, mit Ausnahme des Medieninstituts der Länder, des FWU mit etwa 50 Mitarbeitenden.

Innovationsdruck

Die Digitalisierungsprozesse üben und übten einen erheblichen Innovationsdruck auf diese Marktbereiche, die Unternehmen und Distributionsstrukturen aus. Der zunehmende Einsatz von digitalen Lernplattformen und Lernmanagementsystemen (LMS) wirkt aktuell zusätzlich als Katalysator, denn beim Lernenden und auf dessen Endgeräten laufen die Medien letztlich zusammen. Dies stellt hohe technische Anforderungen an die Distributionssysteme – so sind Schnittstellen zu LMS als obligatorisch zu betrachten – sowie an die Sicherung der Wahrung der Urheberrechte der Content-Produzenten in Form leistungsfähiger Lizenzverwaltungen und an den Datenschutz der Nutzerinnen und Nutzer. Der Bildungsbereich mit in der Überzahl zu schützenden Minderjährigen stellt hierbei eine besondere Herausforderung dar.

In der Digitalisierung und Verfügbarmachung von Bildungscontent hat der kleinere Marktbereich gegenüber dem Schulbuchmarkt bis dato einen erheblichen Innovationsvorsprung, dessen Hauptursache in einem ungleich größeren Veränderungsdruck liegt. Er begann mit der DVD als digitalem physischen Trägermedium als Nachfolger der VHS-Kassette und des 16mm-Films zeitlich sehr viel früher in den 90er Jahren. Hinzu kamen die zunächst verwirrenden Möglichkeiten für Strukturen und Schachtelungen durch Hypertext per HTML. Und schnell wurde deutlich, der Medieninhalt ist nicht der physische Datenträger.

Ein digitales Bildungsmedium, was ist das?

Bereits 2004, ein Jahr vor Youtubes Gründung – Facebook war noch nicht in Sicht und die Schulbuchverlage verstanden unter einem digitalen Schulbuch eine pdf-Datei – zeigte Friedemann Schuchardt wohin die Reise gehen könnte mit den Digitalmedien. Der damalige Geschäftsführer der Matthiasfilm GmbH, einem Medienproduzenten der evangelischen Kirche, stellte eine sogenannte „DVD educativ“ mit dem Titel „Luther“ vor. Das Multimediaprodukt enthält den kompletten Spielfilm Luther von Eric Till aus dem Jahr 2003, unter anderem mit Joseph Fiennes, Sir Peter Ustinov und Bruno Ganz in Hauptrollen. Der Film ist in voller Länge aber auch einzeln kapitelweise aufrufbar. Jedes Kapitel enthält zudem Fragen, Arbeitsblätter und eine Vielzahl an Zusatzinformationen in Form von Audiodateien und Texten, auch zu historischen Quellen. Interviewsequenzen mit einigen Schauspielern zu ihren Rollen runden das Produkt ab. Luther war ein weit über den Spielfilm hinaus umfassendes Multimediaportrait der Reformationszeit, in Schulen vielfältig in Gänze als auch in Teilen/Modulen einsetzbar in den Fächern Geschichte, Sozialkunde, Philosophie und Religion.

Dem vorangegangen war bei Matthiasfilm ein vergleichbares, jedoch nicht so umfangreiches Produkt: „Das Tagebuch der Anne Frank“, basierend auf dem gleichnamigen Spielfilm von Gareth Davies aus dem Jahr 1987. Das Begleitmaterial dieser DVD enthielt etwa als historisches Highlight eine bis dato unveröffentlichte digitalisierte Version einer kurzen 8mm-Schmalfilmaufnahme aus dem Privatleben von Anne Frank.

Das FWU in Grünwald bei München hatte da schon eine Pilot-Produktion mit dem Titel „Die Alpen“, basierend auf dem Träger CD-ROM präsentiert, ein Multimediaprodukt rund um die Alpen, das die unterschiedlichen Aspekte dieser geographischen Region, von der Ökologie über die Landwirtschaft bis hin zum Tourismus, für den Erdkundeunterricht beleuchtete. Die Struktur des Mediums entsprach in etwa der einer Mindmap mit netzartigen Verknüpfungen.

Heute gibt es eine Vielzahl von unterschiedlichsten multimedialen Produkten zu allen schulischen Themen; von „Was ist Zeit?“, einem Grundschulmedium für den Sachunterricht, über „Die französische Revolution“, „Atombau und Atommodelle“, „Proteinbiosynthese“, „Gesunde Ernährung“ bis hin zu „Fake News“ – alle ausgestattet mit zahlreichen Begleitmaterialien und mit einer thematischen Tiefe, die von entsprechenden Kapiteln in Schulbüchern nur selten erreicht wird. Durch den Wegfall der Schuljahresrhythmiken und Drucklegungen im Produktionsprozess weisen diese Medien gegenüber den

Schulbüchern oft auch eine erheblich höhere Aktualität auf.

NRW: Digitales Intermezzo mit Lexikon

Was dementsprechend deutlich verwirrt, sind Entscheidungen, wie sie in diesem Jahr exemplarisch vom Schulministerium in Nordrhein-Westfalen getroffen wurden: Als das Ministerium für Schule und Bildung des Landes NRW am 18. Februar 2021 bekannt gab, dass es 2,6 Millionen Euro „für mehr digitale Lernmittel an den Schulen" ausgebe, darunter für 1,6 Millionen Euro eine Drei-Jahres-Lizenz des Online-Lexikons Brockhaus für alle Schulen in NRW, löste dies sowohl auf Twitter als auch in der Presse Verwunderung aus. Im Deutschlandfunk wurde etwa die Frage gestellt: „Viel Geld für Bildung ohne Nachhaltigkeit?"[7]

In Zeiten von frei verfügbaren Quellen wie Wikipedia, Klexikon und vielfältigen Übersetzungswerkzeugen ist der Erwerb einer zeitlich auf drei Jahre begrenzten Lizenz ganz sicher merk- und fragwürdig. Aber die auf Twitter und andernorts vielfach hingeworfene Forderung nach uneingeschränkter Förderung von OER ist es ebenso, wie das Beispiel Jointly und die beiden Suchmaschinen zeigen. Hier ist ein genauer Blick auf die Angebote besser.

Eine mögliche Zukunft – Distanzlernen, digitale Medien und politisches Wollen

Ein Digitalpakt Schule, der den Namen wirklich verdient, muss die Bereitstellung digitaler Bildungsinhalte für Schulen und die Förderung ihrer Produktion zum integralen Bestandteil einer gemeinsamen Strategie von Bund, Ländern und Kommunen machen. Diese sollte nicht nur das Ausstattungsproblem adressieren und sich wie BMBF und KMK es tun, darauf beschränken, gleich zwei Suchmaschinen für OER-Materialien zu fördern und zu hoffen, dass die OER-Inhalte quasi von selbst entstehen.

Es sollten Nägel mit Köpfen gemacht werden. Das könnte heißen: Unternehmen werden gefragt – diejenigen, die alle Rechte auch an den internen Bild-, Audio-, Text- und Videobestandteilen ihrer Medien halten – , was es denn kosten würde eines ihrer Medien unter eine CC-Lizenz zu stellen und es damit zu einem bundesweit frei verfügbaren OER-Bildungsmedium zu machen. Selbstverständlich hätte das seinen Preis, denn es entspricht einem kompletten Buy-Out des Mediums. Auf der Basis solcher Quellen und mit diesen Quellen als mediale Knetmasse könnten Lehrkräfte aber dann – selbstverständlich unter Einhaltung der Zitationsregeln und der Anerkennung fremder Urheberschaften (CC-BY-SA) – weitere OER-Medien und Lernprojekte zum jeweiligen Thema produzieren und frei zur Verfügung stellen. Und so ganz nebenbei würden dadurch auch übergreifende Kooperationen zwischen Lehrkräften angeregt, eine bundesweit offene Szene, ein virtueller Makerspace für Bildungsmedien. Die OER-Trefferlisten in MUNDO und WLO sähen dann in wenigen Jahren völlig anders aus.

Und wie bewerten wir, was gefördert und gekauft werden soll? Erstens leistet sich das Bundesland Baden-Württemberg seit Jahren eine 40-köpfige Fachkommission zur Bewertung solcher Titel. Zweitens gibt es seit Jahren den Comenius-EduMedia-Award. Man muss solche Entscheidungsgremien nur deutlich ausbauen, anpassen und aufbohren. Das könnte ebenfalls für mehr verfügbare Inhalte sorgen.

Und wo findet man eigentlich diese mehrfach erwähnten Landesportale, diese Landesinfrastrukturen, die bereits ihre Lager füllen? Zwei Forderungen der KMK lauten ja „1. allgemeine Auffindbarkeit von Bildungsmedien" und „4. öffentliche Dokumentation". Eine Lösung dazu wäre also zum Beispiel die Erstellung einer einfachen Linkliste auf einer an zentraler Stelle gehosteten Webseite mit guter Sichtbarkeit. Das fiele – als Kooperation der Länder – in den natürlichen Aufgabenbereich der KMK. Dort findet man aber tief versteckt in der Website hinter dem Begriff „Distanzlernen"[8] nach Bundesländern sortiert nur eine Liste unterschiedlicher Services, einen wilden Mix aus diversen Plattformen und Projekten mit unterschiedlichsten Funktionen. Von da aus muss man sich länderweise durchklicken. Medienrepositorien? Fehlanzeige. Hier müsste also die KMK ihren eigenen Forderungen nachkommen und etwas aufsetzen.

Zum Stichwort Föderalismus bleibt – wie schon am Anfang erwähnt – zu ergänzen: Zugrunde liegt hier nach meiner Auffassung in erster Näherung ein Kommunikationsproblem. Das Kommunikationsproblem ließe sich durch eine klar ausformulierte Medien-Strategie sicherlich besser beheben, an einem runden Tisch mit der KMK und dem Bundesministerium für Bildung und Forschung. Die vielen verschiedenen Portale, Suchmaschinen und Anbieter könnten dann richtig zusammengeführt und für Lehrkräfte und Lernende gewinnbringend geöffnet werden.

Ein sachproblemorientierter großer runder Tisch ohne persönliche oder parteipolitische Eitelkeiten wäre vonnöten, um Medienportale stringent aufzubauen, auszustatten und zu vernetzen. Die Zukunft unserer Schulen, unserer Kinder, unserer Gesellschaft, sollte uns das wert sein.

1 Dieser Artikel ist als Bestandteil der Artikelserie „Schule digital" auf heise.de, https://heise.de/-5993043, am 30.04.2021 unter https://heise.de/-6008139 veröffentlicht worden und wird mit freundlicher Genehmigung des Autors wie auch des heise Verlags hier abgedruckt.

2 https://www.heise.de/news/Schulplattform-Betreiber-Bei-uns-kommt-aus-dem-Digitalpakt-nichts-an-5076231.html

3 https://www.tagesspiegel.de/wissen/mundo-und-wirlernenonline-zwei-plattformen-sind-eine-zu-viel/26845814.html

4 https://www.kmk.org/fileadmin/pdf/PresseUndAktuelles/2018/Digitalstrategie_2017_mit_Weiterbildung.pdf

5 https://www.deutschlandfunk.de/digitale-unterrichtsmaterialien-bildungsportal-mundo-im.680.de.html?dram%3Aarticle_id=484365

6 https://dip21.bundestag.de/dip21/btd/19/224/1922477.pdf

7 https://www.deutschlandfunkkultur.de/digitale-lehrmittel-in-nrw-viel-geld-fuer-bildung-ohne.1264.de.html?dram%3Aarticle_id=493216

8 https://www.kmk.org/themen/bildung-in-der-digitalen-welt/distanzlernen.html

Professor Ulrich Kelber

Sündenbock Datenschutz – Argumente gegen das reflexartig bemühte Standardargument

Gastbeitrag BfDI in DANA – Corona, Warn-App und Datenschutz

Glaubt man den Aussagen mancher Spitzenpolitiker oder Talkshow-Teilnehmer, so wäre die Corona-Pandemie längst im Griff, wäre da nicht dieser lästige Datenschutz, der alles bremst und blockiert. Sogar den raschen Fortgang der Impfungen soll der Datenschutz verhindern, nicht etwa die zu geringe Zahl verfügbarer Impfdosen.

Als Bundesbeauftragter für den Datenschutz berate und begleite ich seit nunmehr einem Jahr zahlreiche Projekte rund um die Bekämpfung der Pandemie. Keine einzige, konkrete und realisierbare Maßnahme der Bundesregierung ist in dieser Zeit aus Gründen des Datenschutzes nicht umgesetzt worden. Für die oft in Debatten geäußerte Behauptung, der Datenschutz stünde der Pandemiebekämpfung im Wege, gibt es keinerlei Belege, sie ist aber toxisch. Zum einen wird damit das notwendige Vertrauen der Bürgerinnen und Bürger in ihr eigenes Grundrecht torpediert. Zum anderen soll dadurch wohl häufig nur von den eigentlichen Defiziten in der Pandemiebekämpfung abgelenkt werden. Darüber hinaus wird verkannt, dass der Datenschutz sehr wohl in der Pandemie deutliche Einschränkungen erfahren hat. Das zeigen beispielsweise der Blick in die Änderungen des Infektionsschutzgesetzes und alle derzeitigen Verfahren der Kontakterfassung, sei es beim Einkaufen oder in den geöffneten Museen.

Impfen

Beim Start der Impfungen gegen das Corona-Virus ist in den vergangenen Wochen medial in einigen Bundesländern der Eindruck vermittelt worden, der Datenschutz verhindere, dass die Angehörigen der jeweiligen Impfgruppen über den Impfstart und die Möglichkeit der Anmeldung informiert würden. Das ist schlichtweg falsch! Statt meine Kolleginnen und Kollegen aus den Ländern in die Planungen einzubinden und sich von ihnen beraten zu lassen, wurden so absurde Wege gewählt, wie die Suche nach Vornamen, die vermeintlich nur von über Achtzigjährigen getragen werden. Den Datenschutz-Fachleuten wurde noch nicht einmal die Gelegenheit gegeben die verschiedenen, datenschutzrechtlich unbedenklichen Möglichkeiten, für die Impfbenachrichtigungen auf die vorhandenen Meldedaten zuzugreifen, darzulegen.

Corona Warn App

Die Erfahrung zeigt: Die Akzeptanz von Maßnahmen wächst, wenn sie in Bezug auf den Schutz persönlicher Daten vertrauenswürdig sind. Die Bürgerinnen und Bürger wollen ihren Beitrag zur Eindämmung der Pandemie leisten, aber nicht dabei durch den Staat oder Internetkonzerne überwacht werden.

Zu Beginn der Beratungen über die Architektur einer Corona Warn App hat mein Haus gesagt: Das muss man anders machen. Zum Beispiel, als ganz am Anfang der Pandemie Mobilfunkzellendaten verwendet werden sollten, um herauszufinden, wer wem begegnet ist. Da haben wir in der Tat unser Veto eingelegt, wenn man das so nennen will. Auch, weil die Funkzellenauswertung für diesen Zweck überhaupt nicht geeignet ist, weil die Genauigkeit oft auf einige hundert Meter begrenzt ist und trotzdem Bewegungsprofile aller Bundesbürger erstellt würden. Das Ergebnis der Zusammenarbeit war eine App, die ein hohes Maß an Vertrauen genießt und mittlerweile mehr als 27 Millionen Mal heruntergeladen wurde.

Natürlich hätte diese App schon frühzeitig weiterentwickelt werden können, mit dem Kontakttagebuch ist das auch schon geschehen. Die sogenannte Cluster-Erkennung oder Check-in-Lösungen sind in Kürze weitere Möglichkeiten, die angeboten werden – datenschutzfreundlich implementiert. Wichtig ist aber die Einsicht, dass eine App allein, egal wie sie ausgestaltet ist, nicht der Heilsbringer in der Pandemie sein kann. Sie ist ein Baustein in einer Strategie, der seinen Nutzen hat, wenn auch alles andere funktioniert: Das Impfen, das Testen, die Quarantäne, die Kontaktnachverfolgung durch die Gesundheitsämter, die Berechenbarkeit der beschlossenen Maßnahmen. Das und nur das zeigen übrigens die Erfahrungen aus Asien, Australien und Neuseeland.

Ein Grundrecht wie das Recht auf informationelle Selbstbestimmung aus Gründen kurzfristiger medialer Effekthascherei dagegen kaputt zu reden halte ich für brandgefährlich. Stattdessen sollten wir unsere Kräfte und unsere Kompetenzen bündeln, um einen guten Weg aus dieser Pandemie zu finden. Mit Konzentration auf die machbaren und funktionierenden Lösungen. Mein Team und ich stehen dafür bereit.



Bild: iStock.com/Prostock-Studio

Dr. Thilo Weichert

Polizeirechtsreform in Schleswig-Holstein



Bild: iStock.com/janniswerner

Die Diskussion über die Modernisierung des Polizei- und Sicherheitsrechts spielte in der letzten Zeit auf Bundes- und Länderebene eine große Rolle. Damit einher ging und geht fast überall eine Verschärfung der gesetzlichen Regelungen – ein Abbau an Datenschutz und eine Erweiterung der Verarbeitungsbefugnisse der Sicherheitsbehörden (vgl. Schwerpunktheft DANA 1/2018).

Es ist weitgehend unstreitig, dass Gesetze, die nicht mehr der technischen Entwicklung entsprechen, weder im Interesse der Sicherheit noch des Datenschutzes sind. Die Parole muss daher sein: „Novellierung ja, aber Datenschutzabbau nein!" Ein Nachzügler bei der Gesetzgebung war Schleswig-Holstein. Während es in anderen Bundesländern teilweise heftigen Widerstand und eine intensive öffentliche Diskussion gab, trat das „Gesetz zur Änderung polizei- und ordnungsrechtlicher Vorschriften im Landesverwaltungsgesetz (LVwGPORÄndG)" fast geräuschlos am 19.03.2021 in Kraft.

Wir durften gespannt sein: Im Koalitionsvertrag der Jamaika-Koalition vom Juni 2017 im nördlichsten Bundesland hatten CDU, Grüne und FDP Folgendes vereinbart: „Das zurzeit geltende Polizeirecht im Landesverwaltungsgesetz werden wir in enger Zusammenarbeit mit anerkannten Polizeirechtsexpert*innen unverzüglich einer Schwachstellenanalyse unterziehen, um Handlungsnotwendigkeiten, insbesondere im Bereich der Terrorismusbekämpfung und in Fällen der organisierten Kriminalität, zu identifizieren." Die Erfahrungen mit Sicherheitsgesetzen der CDU sind, dass diese regelmäßig von Verfassungsgerichten aufgehoben bzw. repariert werden müssen. Aber auch die Erfahrungen mit grün-gelben Regierungsbeteiligungen, etwa in Baden-Württemberg und Hessen (Grüne) oder in Nordrhein-Westfalen (FDP) sind aus Datenschutzsicht ernüchternd und enttäuschend, weil den Verarbeitungswünschen der Sicherheitsbehörden wegen des Nachdrucks der CDU immer wieder entsprochen wurde. Immerhin steht im Kieler Koalitionsvertrag: „Änderungen der Sicherheitsgesetze werden die Koalitionspartner*innen nur im Konsens vollziehen."

- Der Gesetzgebungsprozess

Die politische Diskussion um das Polizeirecht in Schleswig-Holstein begann aus Datenschutzsicht wenig Erfolg versprechend: Das Innenministerium des Landes legte im Dezember 2018 keine

„Schwachstellenanalyse von anerkannten Polizeirechtsexpert*innen“ vor, sondern eine „Wünsch-Dir-was-Liste“ aus der Polizeiabteilung mit 17 Änderungsvorschlägen zum Landesverwaltungsgesetz (LVwG), in dem das Polizeirecht des Landes geregelt ist. In dieser Liste fanden sich so problematische Punkte wie die Vorratsdatenspeicherung, die Quellen-Telekommunikationsüberwachung (TKÜ), die Online-Durchsuchung, verdachtsunabhängige Kontrollen in der Grenzregion, die elektronische Fußfessel sowie außerhalb des Bereichs der Datenverarbeitung der Einsatz von Tasern, der sog. „finale Rettungsschuss“ und der Schusswaffeneinsatz gegen Kinder.

Für die weitere Diskussion war es nicht unbedeutend, welchen Widerstand es gegen Polizeirechtsverschärfungen in anderen Bundesländern gab, namentlich in Bayern, Nordrhein-Westfalen und Niedersachsen. Zwar gab es auch in Schleswig-Holstein dann einige wenige Proteste, die sich aber zahlenmäßig im unteren zweistelligen Bereich bewegten. Im Sommer 2019 erfolgte eine erste grundsätzliche Einigung der Jamaika-Koalitionäre. Relevant war, dass die Verhandlungsführer bei der FDP und den Grünen bürgerrechtliche Positionen vertraten. Diese konnten sich zwar nicht durchgängig durchsetzen und mussten an einigen Stellen mit Bauchschmerzen „Kröten schlucken“. Doch meinte z.B. der grüne Landtagsabgeordnete Burkhard Peters damit leben zu können.

Demgemäß wurde die Debatte über die Polizeirechtsreform im öffentlichen Raum weniger über die Datenverarbeitungsbefugnisse geführt als über den letztlich vorgesehenen sog. finalen Rettungsschuss, der aber nicht von Vorgesetzten angeordnet werden darf, den Schusswaffeneinsatz gegen Kinder oder die Wegweisung bei häuslicher Gewalt.

- Das neue Gesetz

Vorratsdatenspeicherung, Quellen-TKÜ und Online-Durchsuchung konnten vollständig verhindert werden. Bei anderen Streitpunkten konnten deutliche Entschärfungen durchgesetzt werden. So wurde bei der Identitätskontrolle im grenzüberschreitenden Verkehr die im ersten Entwurf vorgesehene „Anlasslosigkeit“ gestrichen und eine Formulierung aufgenommen, mit der explizit ein sog. „racial profiling“ verhindert werden soll (§ 181 LVwG). Mit einem Vorschlag Kontrollquittungen nach Bremer Vorbild auszustellen, konnten sich die Grünen nicht durchsetzen. BodyCams dürfen in Wohnungen nur bei akuter Gefahr und nach Anordnung des Einsatzleiters eingesetzt werden (§ 184a LVwG). Die elektronische Fußfessel darf nur gegen terroristische Gefährder verwendet werden und nicht – wie ursprünglich im Entwurf des Innenministeriums vorgesehen – auch gegen Fußballhooligangs oder andere Rowdies (§ 201b LVwG). Ihr Einsatz soll nach einigen Jahren evaluiert werden.

Die Grünen schreiben sich auf die Fahnen, dass auf ihre Initiative eine ausführliche Regelung zum Einsatz von sog. Vertrauenspersonen aus dem kriminellen Milieu aufgenommen wurde (§ 185c LVwG). Ein parallel zur Diskussion über den Gesetzentwurf laufender parlamentarischer Untersuchungsausschuss zu einer sog. Rockeraffäre hatte deutlich gemacht, dass dieser grundrechtssensible Einsatz von V-Leuten rechtlicher Leitplanken bedarf, die es im Polizeirecht des Landes bis dahin nicht gab.

- Kritik

Nur die oppositionelle SPD stimmte letztlich gegen den Entwurf. Deren Sprecherin Kathrin Bockey bemängelte anlässlich der abschließenden Lesung im Landtag, dass sie bei der V-Leute-Regulierung keinen echten Durchbruch erkennen kann. Bei der Wohnungsverweisung von gewalttätigen Partnern hätte sie sich statt der Dauer von 4 Wochen drei Monate gewünscht (§ 201a LVwG). Die nicht im Landtag vertretene Linke bemängelte, dass Personen künftig ohne Einwilligung Blut abgenommen werden darf, wenn diese Beamte verletzt haben und dabei eine hochinfektiöse Krankheit übertragen haben könnten.

In der Stellungnahme zu dem Entwurf hatte zuvor insbesondere die Gesellschaft für Freiheitsrechte e.V. (GFF) verfassungsrechtliche Bedenken geäußert. Der Jurist Bijan Moini monierte die Regelungen zur Bewegungsbeschränkung von „Gefährdern“ und die damit verbundene Vorverlagerung der Eingriffsrechte. Diese Kritikpunkte zeigen, dass es um Einzelheiten ging, und nicht um die Grundsatzdiskussion über den Präventivstaat, für den Maßnahmen wie Online-Durchsuchung und Vorratsdatenspeicherung stehen.

- Fazit

Die Polizeirechtsreform in Schleswig-Holstein ist bemerkenswert: Waren die Diskussionen in den anderen Bundesländern sowie auf Bundesebene regelmäßig von den informationellen Befugnissen der Polizei geprägt, so lag im nördlichsten Bundesland der Schwerpunkt bei „klassischen“ Fragen des Polizeirechts – der Anwendung unmittelbaren Zwangs. Dass die informationellen Befugnisse letztlich weitgehend akzeptiert wurden – allenfalls beim BodyCam-Einsatz in Wohnungen gab es markante Abweichungen, liegt möglicherweise am Kompromiss, der parteiübergreifend gesucht und gefunden wurde. Dieser Kompromiss machte es letztlich sogar Teilen der Opposition – nicht nur der dänischen Minderheit des SSW, sondern auch der AfD – möglich dem Gesetz zuzustimmen. Die Akzeptanz mag auch darauf zurückzuführen sein, dass vom Bundesverfassungsgericht inzwischen genug Entscheidungen vorliegen, über welche die Grenzen zwischen verfassungsrechtlich noch Zulässigem und polizeilich Gewünschtem als ausgelotet angesehen werden können. Dass diese Rechtsprechung in anderen Bundesländern nicht zur Befriedung geführt hatte, liegt wohl am Symbolgehalt des Polizeirechts, das als Instrument eines „starken Staates“ verstanden wird. Die Debatte über den „starken Staat“ spielt in Schleswig-Holstein schon seit Längerem keine wichtige Rolle im politischen Diskurs.

Dennoch: Der Gewinn an Ausgewogenheit in dem Gesetz wird erkauft durch einen Verlust an textlicher Klarheit: Der Text des verabschiedeten Gesetzes misst immerhin 20 eng gesetzte Seiten. Die Auslotung des verfassungsrechtlich Zulässigen führten zu vielen materiellen und prozeduralen Bedingungen für – auch informationelle – Eingriffe. Die Aufgabe, solche Gesetze in der Polizeiausbildung zu vermitteln, kann nicht hoch genug eingeschätzt werden.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg – Pressemitteilung vom 07. Mai 2021

Bildungsplattform BW: LfDI rät aufgrund hoher datenschutzrechtlicher Risiken von der Nutzung der geprüften Version von Microsoft Office 365 an Schulen ab – Alternativen sollten gestärkt werden

Hintergründe und Folgen der Empfehlung

Das Kultusministerium hatte vorgesehen, als Teil der Bildungsplattform für Schulen eine speziell konfigurierte Version von Microsoft 365 des US-Software-Herstellers Microsoft zu integrieren, um Lehrern, Schülern und Eltern eine geeignete digitale Infrastruktur für Unterricht und Bildung zur Verfügung zu stellen. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Stefan Brink wurde vom Ministerium gebeten in einem Pilotprojekt zur Einführung dieser Software von Mitte Januar bis Ende März beratend tätig zu sein.

In diesem Rahmen prüfte der LfDI die speziell für den Einsatz im Schulbetrieb konfigurierte Version des Produktes MS 365 in einem Praxistest. Über die hierzu notwendige Technik verfügt der Landesbeauftragte, seit ihm Mittel für ein eigenes Prüflabor vom Parlament zur Verfügung gestellt wurden.

Im Wesentlichen wurde geprüft, ob die in der Datenschutz-Folgenabschätzung (DSFA) des Ministeriums vom Oktober 2020 (Pressemitteilung des Landesbeauftragten „LfDI begleitet Pilotprojekt des Kultusministeriums zur Nutzung von Microsoft Office 365 an Schulen") vorgeschlagenen Abhilfemaßnahmen zur Minimierung der Risiken der Microsoft-Software tatsächlich umgesetzt wurden und sich als ausreichend erwiesen; geprüft wurde auch, welche Datenflüsse beim Pilotbetrieb tatsächlich messbar stattfanden, insbesondere ob unerwünschte beziehungsweise nicht angeforderte Datenverarbeitungen, beispielsweise von Telemetrie-, Diagnose- (oder anders bezeichneten) Daten, erkennbar waren und inwieweit die Verarbeitung personenbezogener Daten von Lehrern und Schülern zu eigenen Zwecken Microsofts festzustellen sind. Im Rahmen dieser Prüfung wurde zudem untersucht, ob Daten in Drittstaaten außerhalb des Geltungsbereichs der DSGVO fließen und ob durch eine sichere verschlüsselte Kommunikation die Möglichkeiten eines Zugriffs seitens des Anbieters oder Dritter wirksam eingeschränkt werden konnten.

Zu den Prüfungen im Praxistest wurden in mehreren Bereichen Stichproben genommen. Während seiner Beratung war der LfDI in regelmäßigem Austausch mit dem Kultusministerium und Vertretern des Software- und Dienste-Anbieters.

Wenngleich die Prüfungen aufgrund des Umfangs und Weiterentwicklung der Dienste nicht abschließend sein konnten, so waren deren Ergebnisse doch hinreichend klar, um eine Empfehlung an das Kultusministerium zu richten.

Der Landesbeauftragte Stefan Brink bewertet die Risiken beim Einsatz der nun erprobten Microsoft-Dienste im Schulbereich als inakzeptabel hoch und rät davon ab diese dort zu nutzen. Der Landesbeauftragte empfiehlt ferner die im Schulbereich vorhandenen Alternativen weiter zu stärken.

„Schülerinnen und Schüler, Eltern und Lehrerinnen und Lehrer wollen digitale und rechtssichere Lösungen für den Unterricht. Wir unterstützen das", so Stefan Brink. Deswegen wurde mit hohem Einsatz im Rahmen des Pilotprojekts versucht Klarheit über Datenflüsse, Rechtsgrundlagen und technische Maßnahmen des Anbieters zu erlangen, was jedoch im Ergebnis nicht zufriedenstellend gelungen sei.

Verantwortliche – und das sind die Schulen (vgl. Artikel 4 Nr. 7 DSGVO) – haben beim gewählten System keine vollständige Kontrolle über das Gesamtsystem und den US-amerikanischen Auftragsverarbeiter. Sie können nach der Bewertung des Landesbeauftragten derzeit nicht ausreichend nachvollziehen, welche personenbezogenen Daten wie und zu welchen Zwecken verarbeitet werden und sie können nicht nachweisen, dass die Verarbeitung auf das für diesen Zweck notwendige Minimum reduziert ist. All das müssten sie aber, um ihrer Rechenschaftspflicht aus Artikel 5 Absatz 2 DSGVO gerecht zu werden. Zudem ist für einige Übermittlungen persönlicher Daten an Microsoft – teilweise auch in Regionen außerhalb der EU – keine Rechtsgrundlage erkennbar, die nach DSGVO aber erforderlich ist. Das gilt insbesondere auch für internationale Datenflüsse im Lichte des Schrems-II-Urteils des Europäischen Gerichtshofs aus dem Jahr 2020.

Für den Schulbereich hat der LfDI daher ein hohes Risiko der Verletzung von Rechten und Freiheiten betroffener Personen festgestellt. Dies gilt für die ins Auge gefasste Erweiterung des Systems um Konten für die Schülerinnen und Schüler umso mehr. Der Staat hat eine Garantenstellung für die in der Regel minderjährigen Schülerinnen und Schüler, welche zudem der staatlichen Schulpflicht unterliegen und daher der Verwendung ihrer persönlichen Daten nicht ausweichen können. In dieser Konstellation bewertet der Landesbeauftragte das Risiko der eingesetzten Software als inakzeptabel hoch.



Bild: shutterstock.com/Tada Images

LfDI Brink: „Es erscheint zwar nicht gänzlich ausgeschlossen mit anderen Varianten der im Pilotversuch genutzten Produkte und unter wesentlich modifizierten Einsatzbedingungen damit im Schulbereich rechtskonform zu arbeiten. Es ist in den vergangenen Monaten auch nach intensiver Zusammenarbeit und mit hohem Personaleinsatz aber nicht gelungen eine solche Lösung zu finden." Angesichts dieses Ergebnisses erscheint es mehr als fraglich, ob es den für die Datenverarbeitungen verantwortlichen Schulen, auch mit Unterstützung durch das Kultusministerium, in absehbarer Zeit gelingen kann die getesteten Produkte rechtssicher zu nutzen.

Aus Sicht des LfDI hat eine Bildungsplattform durchaus weiter Zukunft. Sie könnte beispielsweise aus unterschiedlichen Tools wie zum Beispiel Big Blue Button und Moodle bestehen, die bereits jetzt intensiv von den Schulen im Land genutzt werden. Da diese vom Land selbst betrieben werden, liegen damit zahlreiche im Pilotprojekt festgestellte Risiken hier prinzipiell nicht vor.

Der Landesbeauftragte wird vor den Sommer-Schulferien aus eigener Initiative keine Prüfungen in Schulen mit der Zielsetzung einer Untersagung von Produkten vornehmen. Ab dem Beginn des neuen Schuljahres jedoch wird die Behörde allen dann vorliegenden Beschwerden mit Nachdruck nachgehen.

Für alle übrigen öffentlichen und privaten Nutzer solcher Software gelten weiterhin die vom Landesbeauftragten insbesondere in seiner Handreichung „Schrems II – Was jetzt in Sachen internationaler Datentransfer?" dargestellten Maßgaben, die auf der Homepage des Landesbeauftragten abrufbar ist: Alle Verantwortlichen müssen eine Risikobewertung mit Blick auf die konkret verarbeiteten Daten vornehmen und sich nachvollziehbar mit den Rechtsgrundlagen ihrer Datenverarbeitungen befassen. Diese Rechtsgrundlagen unterscheiden sich im öffentlichen und privaten Sektor zum Teil erheblich, so können Behörden grundsätzlich keine Daten auf Basis eines ‚berechtigten Interesses' verarbeiten und sind auch bei der Nutzung von Einwilligungen eingeschränkt. Der LfDI betont dabei, dass bei dieser Betrachtung pauschale Aussagen wie etwa, dass eine Software immer oder nie datenschutzkonform einsetzbar sei, zu undifferenziert und nicht überzeugend sind. Beim Einsatz außereuropäischer Anbieter ist auch stets zu prüfen, ob es Alternativen gibt, die eine weniger risikoreiche Verarbeitung ermöglichen.

Weitere Informationen:

Das Kulturministerium hat das Pilotprojekt initiiert und den Projektgegenstand und -zeitlauf bestimmt. Etwa 3 Monate dauerte die Praxisprüfung. Bereits vorher hat der LfDI verschiedene Prüfungen durchgeführt, unter anderem im Kontext der zweiten Datenschutz-Folgenabschätzung des Kultusministeriums. Diese Prüfungen des LfDI dienten unter anderem dazu mögliche Risiken zu identifizieren und frühzeitig Abhilfemaßnahmen zu schaffen. Nach der Pilotphase hat der LfDI die Ergebnisse ausgewertet und in einer Stellungnahme eine Empfehlung an das für die Bildungsplattform zuständige Ministerium abgegeben. Der LfDI war beratend im Pilotprojekt tätig, in diesem Rahmen trifft er keine Anordnungen und spricht keine Untersagungen aus. Diese Beratungstätigkeit ist mit der Beendigung des Piloten abgeschlossen.

Offener Brief an das europäische Parlament



Sehr geehrte Abgeordnete des Europäischen Parlaments,

die unterzeichnenden Organisationen fordern das Europäische Parlament nachdrücklich auf ein hohes Niveau an Datenschutz und Vertraulichkeit in der geplanten ePrivacy-Verordnung zu gewährleisten und die Schwächen der aktuellen Position des Rates während der Trilogverhandlungen zu beheben.

Vor vier Jahren schlug die Europäische Kommission die Datenschutzverordnung für elektronische Kommunikation (ePrivacy Regulation/-Verordnung) vor, um die von der DSGVO begonnene Modernisierung des EU-Datenschutzrahmens abzuschließen. Um die Bedenken hinsichtlich der Verwendung von Cookies und anderen Tracking-Technologien auszuräumen, hat das Europäische Parlament folgende Bestimmungen beschlossen:

- Der Schutz von Internetnutzern vor Tracking und Überwachung, sei es durch Cookies oder andere technische Mittel. Das Sammeln oder Speichern von Daten auf dem Gerät eines Benutzers ist nur mit Zustimmung des Benutzers gestattet, es sei denn, dies ist für den Dienst technisch erforderlich (Artikel 8).
- Das Verbot von Tracking- oder Cookie-Walls, die Benutzer dazu zwingen sollen, der Verarbeitung oder Speicherung zusätzlicher Daten im Austausch für den Zugriff zuzustimmen (Artikel 8).
- Die Entlastung der Internetnutzer durch technische Datenschutzeinstellungen, mit denen sie die Auswahl von Einwilligungen automatisieren und rechtsverbindliche Signale von Hardware oder Software verwenden können, die an die Webseite übermittelt werden (Artikel 9 und 10). Artikel 19 legte ein Verfahren für die Spezifikation solcher Signale durch die Europäische Datenschutzbehörde fest.

Diese Schutzmaßnahmen wurden vom Rat in seinem Verhandlungsmandat beseitigt oder geschwächt. Artikel 8 Abs. 1 Buchstaben a, c und d des Rates schaffen Unklarheiten über die für einen Dienst „technisch erforderlichen" Daten und öffnen die Tür für das Tracken von Nutzern. Darüber hinaus wurde das Verbot von „Tracking-Walls" in einen Erwägungsgrund verschoben und unter unklare Vorbehalte gestellt.

Der Rat hat auch die Artikel 9 und 10 gestrichen und sich von den technischen Lösungen und den Forderungen von Zustimmungslösungen bei Datenerfassung abgewandt. Infolgedessen müssen sich Benutzer den anhaltenden Belästigungen durch Zustimmungsbanner stellen, die versuchen sie mit „Dark Pattern" (unethischen Webseitenmustern) zu manipulieren. Anstelle solcher Anfragen könnten rechtsverbindliche Signale treten, die vom Benutzer konfiguriert wurden. Diese Lösung bleibt jedoch nun Wunschdenken und wird in einen Erwägungsgrund verwiesen. In Bezug auf das „Privacy by Design" (datenschutzfreundliche Gestaltung) und „Privacy by Default" (Datenschutz durch Voreinstellung) haben sich die meisten Browser dem Schutz ihrer Benutzer verschrieben. Diese Entwicklung wird in der Verordnung nicht aufgegriffen; diese sollte vielmehr berücksichtigt werden.

Seit das Parlament im Oktober 2017 seinen Standpunkt festgelegt hat, wurde das Vertrauen der Öffentlichkeit in die Internetdatenverarbeitung durch den Skandal von Cambridge Analytica beeinträchtigt. Von der ePrivacy-Verordnung muss die klare Botschaft ausgehen, dass die Zukunft eher Geschäftsmodellen gehört, die Grundrechte und Innovation vereinen, als solchen, die ein personalisiertes Fahndungssystem betreiben.

Der Standpunkt des Rates legitimiert stattdessen Missbräuche und Verstöße gegen das Datenschutzrecht und geht nicht auf das Vertrauensdefizit ein. Im Jahr 2016 stellte eine Eurobarometer-Umfrage fest, dass „mehr als sieben von zehn Internet- und Online-Plattformbenutzern der Meinung sind, dass sie über die im Internet über sie gesammelten Daten besorgt sind". Im Jahr 2020 haben Studien ergeben, dass ein Drittel der Verbraucher auf diese Bedenken reagiert und bei mindestens einem Unternehmen aus Datenschutzgründen den Kontakt beendet hat. Dieselbe Studie ergab, dass weitere 87% der Befragten besorgt waren, dass ihre Daten aufgrund der COVID-19-Pandemie nicht durch die Tools geschützt werden, die sie für die Arbeit im Homeoffice benötigen.

Wir fordern das Europäische Parlament nachdrücklich auf seine Position zu bekräftigen und sicherzustellen, dass die ePrivacy-Verordnung ihre Ziele erreicht. Personenbezogene Daten im Bereich der elektronischen Kommunikation sind äußerst sensibel, da sie intime Aspekte des Privatlebens von Einzelpersonen offenlegen, insbesondere wenn jetzt während der COVID-19-Pandemie alltägliche Aktivitäten und Austausch großteils online stattfinden. Der durch die DSGVO gewährte Schutz sollte daher ergänzt werden, indem Lücken geschlossen und Grauzonen aufgehellt werden, die von der Trackingbranche weitgehend missbraucht wurden, sowie indem zusätzliche, stärkere Garantien

für die Verarbeitung personenbezogener Daten in diesem Bereich geschaffen werden.

Wir fordern das Europäische Parlament auf die Stellungnahmen des Europäischen Datenschutzausschusses und des Europäischen Datenschutzbeauftragten umfassend zu berücksichtigen und Vorschläge oder Kompromisse abzulehnen, die das Schutzniveau der DSGVO und der aktuellen Datenschutzrichtlinie für elektronische Kommunikation verringern würden.

Mit freundlichen Grüßen

Dear Members of the European Parliament

The undersigned organisations urge the European Parliament to ensure a high level of protection of privacy and confidentiality in the upcoming ePrivacy Regulation and to address the weakness in the current Council position during trilogue negotiations.

Four years ago, the European Commission proposed the ePrivacy Regulation to complete the modernisation of the EU data protection framework begun by the GDPR. To address the concerns related to the use of cookies and other tracking technologies, the European Parliament adopted several provisions that:

- Protect Internet users from tracking and monitoring, whether by cookies or other technological means. The collection of data from, or storage of data on, a user's device is allowed only with the consent of the user unless technically required for the service (Article 8);
- Prohibited tracking or cookie walls, which seek to coerce users into 'consenting' to the processing or storage of additional data in exchange for access (Article 8)
- Lightened the burden of privacy controls on Internet users, by allowing them to automate consent choices and use legally binding signals sent by network-connected software or hardware to communicate them to websites (Articles 9 and 10). Article 19 set out a process for the specification of such signals by the European Data Protection Board.

These protections were removed or weakened by the Council in its negotiation mandate.

The Council's Article 8(1) letters a, c and d create ambiguity about the data that are "technically necessary" for a service and open the door to the tracking of users. Furthermore, the prohibition against "tracking walls" has been moved to a Recital and qualified with unclear caveats.

Council also deleted Articles 9 and 10, backing away from technical solutions to the constant requests to agree to further data collection. As a consequence, users will have to face the continued nuisance of consent banners which try to manipulate them with 'dark patterns'. These requests could instead be dealt with by legally binding signals configured by the user, but this solution has now been abandoned to wishful thinking and relegated to a Recital. As regards privacy by design and default, most browsers have shifted to protecting their users, an evolution which the Regulation has not taken account of and should expand on.

Since the Parliament agreed its position in October 2017, public trust in data collection has been damaged by the Cambridge Analytica scandal. The ePrivacy regulation must send a clear message that the future belongs to business models which unify fundamental rights and innovation, rather than those who operate a personal data dragnet.

The Council position, instead, legitimises abuses and breaches of data protection law and fails to address the trust deficit. In 2016, a Eurobarometer survey found that "more than seven in ten Internet and online platform users agree they are concerned about the data collected about them on the Internet". In 2020, studies have found that a third of consumers acted upon these concerns, and terminated their relationship with at least one business because of data privacy concerns. The same study found that another 87% of respondents was worried about their data not being protected by the tools they need to use for remote working because of the COVID-19 pandemic.

We urge the European Parliament to reassert their position and ensure that the ePrivacy Regulation delivers on its objectives. Personal data in the field of electronic communications are extremely sensitive, as they reveal intimate aspects of the private life of individuals, particularly during the COVID-19 pandemic when everyday activities and exchanges are now largely happening online. Therefore, the protection afforded by the GDPR should be complemented by closing loopholes and grey areas that have been widely abused by the tracking industry, as well as by providing additional, stronger guarantees to personal data processing in that field.

We call on the European Parliament to take full account of the opinions of the European Data Protection Board and the European Data Protection Supervisor, and to reject any proposal or compromise that would lower the level of protection provided by the GDPR and the current ePrivacy Directive.

Yours sincerely,

Access Now, International • Amnesty International • BEUC, The European Consumer Organisation • Bits of Freedom, The Netherlands • Centre for Peace Studies, Croatia • Civil Liberties Union for Europe (Liberties), International • Civil Rights Defenders, Sweden • Coalition for Civil Liberties and Rights, Italy • Communia, International • Deutsche Vereinigung für Datenschutz e.V. (DVD), Germany • Digitalcourage, Germany • Electronic Frontier Foundation, International • Free Knowledge Advocacy Group EU, International • Homo Digitalis, Greece • Human Rights Monitoring Institute, Lithuania • Hungarian Civil Liberties Union, Hungary • Institute of Information Cyprus, Cyprus • IT-Pol Denmark, Denmark • Liga lidských práv | League of Human Rights, Czech Republic • Ligue des Droits Humains, Belgium • Netzwerk Datenschutzexpertise, Germany • Open Rights Group, United Kingdom • Panoptykon Foundation, Poland • Platform Bescherming Burgerrechten, The Netherlands • Privacy First, The Netherlands • Privacy International, International • Ranking Digital Rights, USA • The Irish Council for Civil Liberties, Ireland • The Privacy Collective, International • Xnet, Spain


Von den Jahren 2014 und 2015 sind noch alle Hefte in großer Anzahl verfügbar
Bestellbar für 4 Euro pro Jahrgang oder 6 Euro für beide Jahrgänge *
Datenschutz Nachrichten
1/2014 Konzern-Datenschutz
2/2014 Das Internet der Dinge
3/2014 Datenschutz im Reiseverkehr
4/2014 Big Data
Datenschutz Nachrichten
1/2015 Mobilität, Telematik und Datenschutz
2/2015 Datenerfassung und Flüchtlinge
3/2015 Rote Linien zur EU-DSGVO
4/2015 Sichere Häfen
* Nur solange der Vorrat reicht

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Anti-Hass-Gesetz in Kraft

Bundespräsident Frank-Walter Steinmeier hat die zurückgehaltenen Gesetze gegen Hass und Rechtsextremismus mit einer Regelung zur Bestandsdatenauskunft unterzeichnet und in Kraft gesetzt. Bundesjustizministerin Christine Lambrecht äußerte sich erleichtert, dass die Normen, mit denen Hass und Hetze im Internet bekämpft werden sollen, nach Verzögerungen und Auseinandersetzungen in veränderter Form wirksam werden können. Die Initiative diene „dem Schutz aller Menschen, die im Netz bedroht und beleidigt werden". Künftig könnten Polizei und Justiz sehr viel entschiedener gegen menschenverachtende Hetze vorgehen: „Wir erhöhen die Abschreckung und den Ermittlungsdruck deutlich."

Das Gesetzespaket besteht aus dem „Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität", das am 03.04.2021 in weiten Teilen in Kraft trat, sowie dem ab dem 02.04.2021 geltenden „Gesetz zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020".

Bundespräsident Frank-Walter Steinmeier hatte sich nach der Ansage der Karlsruher Richter zunächst Anfang Oktober geweigert, das vom Bundestag bereits im Juni 2020 beschlossene Anti-Hass Gesetz zu unterzeichnen. Es enthält weitgehende Vorschriften zur Herausgabe von Bestandsdaten inklusive Passwörtern. Der Bundestag verabschiedete daraufhin Ende Januar die Reform der Bestandsdatenauskunft, um damit auch das Gesetz gegen Hass und Hetze zu „reparieren" (DANA 1/2021, 36 f.). Der Bundesrat stimmte dem Entwurf Mitte Februar aufgrund zahlreicher rechtlicher Einwände aber nicht zu, sodass die Bundesregierung den Vermittlungsausschuss zwischen beiden Gremien anrief.

Dieser verständigte sich auf einen Kompromiss. Eine Passwortherausgabe kommt demnach nur noch bei bestimmten, besonders schweren Straftaten in Betracht. Die Vertreter von Bund und Ländern schränkten zudem die Abrufmöglichkeit für Nutzungsdaten wie URLs, Kommunikation auf sozialen Netzwerken und Pseudonymen ein.

Steinmeier unterzeichnete beide Gesetze daraufhin am 30.03.2021, am 01.04.2021 wurden sie im Bundesgesetzblatt verkündet. Mit dem Anti-Hass-Gesetz wird das Strafgesetzbuch erweitert und verschärft. Schon das „Billigen" oder Androhen von Straftaten etwa in sozialen Netzwerken gilt als Verbrechen, wenn entsprechende Äußerungen geeignet sind, den öffentlichen Frieden zu stören. Drohungen mit Taten gegen die sexuelle Selbstbestimmung, die körperliche Unversehrtheit, die persönliche Freiheit oder gegen Sachen von bedeutendem Wert, die sich gegen die Betroffenen oder ihnen nahestehende Personen richten, werden ebenfalls strafbar.

Wer öffentlich im Netz andere beleidigt, dem drohen bis zu zwei Jahre Haft. Den Katalog der rechtswidrigen Inhalte im Netzwerkdurchsetzungsgesetz hat der Gesetzgeber um das Delikt der „Verunglimpfung des Andenkens Verstorbener" ergänzt.

Anbieter von Telemediendiensten wie WhatsApp, Google, Facebook, Tinder & Co. müssen sensible Daten von Verdächtigen wie IP-Adressen und Passwörter künftig an Sicherheitsbehörden herausgeben. Dazu kommt eine Pflicht für Betreiber großer sozialer Netzwerke wie Facebook, TikTok und Twitter strafrechtlich relevante Inhalte wie Hassbeiträge, Terrorismuspropaganda oder Bedrohungen und Darstellungen sexuellen Kindesmissbrauchs nicht mehr nur zu löschen, sondern parallel unaufgefordert – zusammen mit aussagekräftigen Internetkennungen inklusive Portnummern – ans Bundeskriminalamt (BKA) zu melden.

Für diese lange besonders umstrittene Bestimmung gilt eine Übergangsklausel bis zum 01.02.2022, damit die Provider und das BKA ihre Prozesse umstellen können. Netzpolitisch aktive Vereine hatten gewarnt, dass dort eine umfassende „Verdachtsdatenbank" in Form eines polizeilichen Zentralregisters entstehe. Die Grünen forderten daher ein entschärftes zweistufiges Verfahren, fanden dafür aber auch im Vermittlungsausschuss keine Mehrheit.

Wegen der Bestandsdatenauskunft hing auch das neue Zollfahndungsdienstgesetz bei Steinmeier fest. Dieses trägt mit den Korrekturen von Bund und Ländern nun ebenfalls die Unterschrift des Bundespräsidenten und trat auch am 02.04.2021 in Kraft. Die Kompetenzen des Zollkriminalamts und der Zollfahndungsämter etwa bei der – auch präventiven – Überwachung der Telekommunikation sowie des Brief- und Postverkehrs hat der Gesetzgeber hier deutlich ausgeweitet. Verbunden ist damit erstmals auch die Befugnis, Staatstrojaner für die Quellen-TKÜ nutzen zu dürfen (Krempl, Gesetze gegen Hass und zur Passwortherausgabe treten in Kraft, www.heise.de 01.04.2021, Kurzlink: https://heise.de/-6004554).

Bund

Stasi-Unterlagen-Behörde geht ins Bundesarchiv über

Der Bundesbeauftragte für die Stasi-Unterlagen (BStU) Roland Jahn hat am 19.03.2021 seinen 15. und letzten Tätigkeitsbericht vorgestellt, den letzten der Behörde überhaupt, bevor sie am 17.06.2021 offiziell mit dem Bundesarchiv verschmolzen wird. Dabei gehen nach 30 Jahren DDR-Aufarbeitung 111 Regalkilometer Stasi-Akten an zunächst 13 und mittelfristig nur noch sechs

Standorten ans Bundesarchiv über. Mehr als drei Milliarden Euro wurden ausgegeben, zu rund vier Fünfteln für Personal. Es wechseln auch rund 1.300 BStU-Mitarbeiterinnen und Mitarbeiter. Das Stasi-Unterlagen-Gesetz gilt weiter, sodass sich am Zugang zu den Akten nichts ändern wird – weder zum Schlechteren noch zum Besseren. Insgesamt 2,17 Mio. Menschen haben seit 1991 rund 3,35 Mio. Anträge gestellt, um zu erfahren, was die DDR-Staatssicherheit einst über sie festhielt. Auch noch Anfang 2021 kommen zwischen 3.000 und 4.500 neue Auskunftsbegehren im Monat. Die Anfragen sind aber rückläufig: Nach ca. 56.000 Anträgen im Jahr 2019 waren es 2020 rund 37.400. Bei rund 20% der Anträge geht es mittlerweile nicht mehr um das persönliche Schicksal, sondern um die Geschichte von Eltern und Großeltern. Vier Millionen weitere Anträge stellten in den vergangenen 30 Jahren Behörden und – viel seltener – private Firmen, die Mitarbeiter auf mögliche Stasi-Verstrickungen überprüfen wollten, Journalisten und Wissenschaftler.

Jahn meinte bei der Vorstellung seines Berichts, die Akten blieben weiterhin sehr wichtig für die Demokratie: „Die Stasi-Unterlagen können unserer heutigen Gesellschaft einen großen Dienst erweisen." Es gehe nicht nur um Vergangenheit. Im Stasi-Unterlagen-Archiv stecke „enorm viel Stoff für die Gestaltung von Demokratie" und für die Sensibilisierung für Werte wie Freiheit und Menschenrechte. Der Vorsitzende der Union der Opferverbände Kommunistischer Gewaltherrschaft (UOKG), Dieter Dombrowskis, erklärte: „Die Arbeit der Stasi-Unterlagen-Behörde ist eine Erfolgsgeschichte, die trotz anfänglicher Skepsis am Ende zu Klarheit und Aufklärung geführt hat." Niemals zuvor in der Weltgeschichte hat sich eine Gesellschaft mit so großem Aufwand an Personal und Geld der Aufgabe gestellt, eine vorangegangene Diktatur und ihre Untaten aufzuklären. Mit „Aufarbeitung" wurde ein vorher ganz anders gemeintes Wort dafür umgewidmet. Der in Bezug auf die Nazi-Zeit gängige Begriff „Vergangenheitsbewältigung" war ja nicht besonders glücklich.

Der 68-jährige Historiker, Journalist und langjährige BStU-Mitarbeiter Christian Booß zieht eine eher kritische Bilanz: „Roland Jahn hat über den Bestrebungen, seine Behörde und seine Funktion abzuwickeln, wichtige interne Reformaufgaben vernachlässigt." Booß setzt sich mit dem Bürgerkomitee 15. Januar e.V. für eine Fortsetzung der Aufarbeitung ein und meint: „Im Vorgriff auf die Übergabe der Behörde an das Bundesarchiv wurde die Geheimdienstforschung faktisch abgewickelt."

• Geschichte des BStU

Die BStU geht zurück auf Debatten im Einheitsjahr 1990 und auf die zeitweilige Besetzung früherer Stasi-Gebäude durch DDR-Dissidenten unter der Parole: „Meine Akte gehört mir!" Die zumeist auf menschenrechtswidrige Weise entstandenen Akten konnten aber nicht an die Betroffenen „ausgegeben" werden, weil in fast allen Unterlagen mehrere, manchmal viele Personen genannt sind. Außerdem sollte auch die deutsche Gesellschaft insgesamt erfahren, wie der Geheimdienst die SED-Herrschaft „abgesichert" hatte.

Trotz des fast immer gewaltfreien Sturmes auf Dienststellen der Stasi im Dezember 1989 wurden noch im Frühjahr 1990 in großem Umfang Akten und elektronische Datenträger der Stasi vernichtet – oft im Einverständnis mit Kontrolleinrichtungen wie dem zentralen Runden Tisch oder den Bürgerkomitees. Mit fadenscheinigen Begründungen waren die unerfahrenen Bürgerrechtler dazu überredet worden, etwa mit der Behauptung, Auslandsspionage betreibe jeder Staat, und jeder Staat müsse die eigenen Spione schützen dürfen.

Nachdem diese Vernichtungen gestoppt waren, blieb Unbehagen über die ungeheuren Materialberge zurück. Sie waren ein wissenschaftlich wertvolles, zugleich aber politisch schwieriges Erbe. Bald kursierte die Befürchtung, eine Offenlegung der Akten könnte zu Selbstjustiz führen, wenn ausgespitzelte Menschen ihre Verräter zur Rede stellen wollten. In Wirklichkeit wurde kein einziger derartiger Übergriff registriert.

Die einzige frei gewählte DDR-Volkskammer legte noch die Grundlage für eine Behörde, die dann nach dem 03.10.1990 vom Bundestag im Stasi-Unterlagen-Gesetz (StUG) legitimiert wurde. Das Gesetz regelt sowohl den Datenschutz wie auch den Aktenzugang. Die in den Beständen der BStU recherchierten Akten wurden und werden auch künftig zu einem angefragten Thema (meist zu einer Person) erst von Mitarbeitern durchgesehen, bevor sie – fast immer fragmentarisch und selbst auf den freigegebenen Seiten noch oft mit geschwärzten Namen und ähnlichen personenbezogenen Informationen – dem Antragsteller vorgelegt werden. Für Kopien aus dem Material gelten mitunter noch schärfere Regeln.

In den 1990er-Jahren, der Amtszeit des ersten Bundesbeauftragten für die Stasi-Unterlagen (und späteren Bundespräsidenten) Joachim Gauck, waren die Vorschriften noch etwas lockerer gehandhabt worden. Als im Jahr 2000 Medien im Zusammenhang mit der in der damaligen CDU-Spendenaffäre Zugang zu Stasi-Unterlagen über Helmut Kohl einforderten, klagte der ehemalige Bundeskanzler dagegen. Nach mehreren Instanzen führte diese Klage zu einer von Gerichten erzwungenen restriktiveren Auslegung des Datenschutzes. Das „Angstschwärzen" wurde in der BStU zum Normalfall, sogar bei Akten aus den 1950er- und 1960er-Jahren, die nach normalem Archivrecht längst ungeschwärzt zugänglich gewesen wären. Einmal machte ein Mitarbeiter allen Ernstes das Wort „Gott" unkenntlich – weil dessen Persönlichkeitsrechte durch das Auftauchen in einem Spitzelbericht der Stasi von 1981 verletzt werden könnten. Die gesamte Amtszeit der zweiten Bundesbeauftragten Marianne Birthler war von diesem deutlich erschwerten Zugang zu den Akten gekennzeichnet. Auch in der Amtszeit des dritten und letzten Bundesbeauftragten Roland Jahn seit 2011 konnte die BStU die bürokratischen Hemmnisse nicht wirklich überwinden, auch wenn vieles besser wurde.

Offen ist nach wie vor der Umgang mit den in rund 16.000 Säcken enthaltenen „vorvernichteten" Stasi-Akten. Für ihre virtuelle Rekonstruktion mittels Scannern standen Millionen bereit, doch das Projekt versandete in Bürokratie und überhöhten Erwartungen. Christian Booß kritisiert: „Die computergestützte Zusammensetzung der zerrissenen Akten, immerhin ein Auftrag des Bun-

destags, ist faktisch tot. Seit fünf Jahren wird gar nichts mehr elektronisch gepuzzelt.“ Die Schnipsel manuell zusammenzusetzen wäre beim bisherigen Tempo wohl eine Aufgabe für mehrere Jahrhunderte (Kellerhof, Selbst der Name „Gott“ wurde geschwärzt – wegen Persönlichkeitsrechten, www.welt.de 19.03.2021; Akten bleiben offen, Kieler Nachrichten 20.03.2021, 3; Weniger Akteneinsicht, SZ 20./21.03.2021, 6).

Bund

Staatliche Mobilfunküberwachung auf hohem Niveau

Gemäß einer Antwort der Bundesregierung auf eine Anfrage der Linksfraktion im Bundestag nimmt die verdeckte Überwachung durch deutsche Strafverfolgungsbehörden gegenüber Mobiltelefon-Nutzern wieder zu. Allein die Bundespolizei hat im Jahr 2020 in 50 Ermittlungsverfahren 101.117 „stille SMS“ verschickt, um Personen zu orten. Das sind mehr als doppelt so viele „Stealth Pings“ als 2019, als der einstige Bundesgrenzschutz 48.000 entsprechende geheime Kurznachrichten aussandte. Die Bundespolizei setzt das umstrittene Instrument damit in etwa wieder so oft ein wie 2018. Die zwischenzeitliche Abnahme der Zahl erklärt sich durch ein Urteil des Bundesgerichtshofs (BGH), der im Februar 2018 für eine Strafverfolgung mit stiller SMS einen richterlichen Beschluss fordert. Dazu der linke Bundestagsabgeordnete Andrej Hunko: „Die BGH-Entscheidung konnte die ausufernde Überwachung bei der Bundespolizei offenbar nur kurze Zeit eindämmen.“

Das Bundeskriminalamt (BKA) hat im Jahr 2020 in 82 Verfahren 44.444 entsprechende heimliche Kurzmitteilungen verschickt, 2019 waren es 41.300. Wie viele Betroffene der Maßnahmen der Polizeibehörden des Bundes nachträglich darüber informiert wurden, ist der Regierung nicht bekannt: Dieser Schritt obliege den jeweils zuständigen Staatsanwaltschaften. Beim Zoll behandelt das federführende Bundesinnenministerium (BMI) die Zahlen zur stillen SMS seit 2012 als Verschlusssache. Beim Bundesamt für Verfassungsschutz (BfV) verfährt das Ressort seit Anfang 2019 genauso. Zuvor hatte der Inlandsgeheimdienst Werte von bis zu 180.000 entsprechenden Abfragen pro Jahr erreicht. Das BMI weigert sich nun auch, Informationen über entsprechende BfV-Aktivitäten in „abstrahierter Form“ zu veröffentlichen. Zu späteren Benachrichtigungen erfolge hier zudem „keine maßnahmenbezogene Erhebung“. Angaben zum Bundesnachrichtendienst gelten ebenfalls als geheim.

Stille SMS adressieren einzelne Mobiltelefone, ohne dem Nutzer angezeigt zu werden. Ihr Gerät meldet sich aber bei der eingebuchten Funkzelle zurück, erzeugt so auswertbare Verbindungsdaten und verrät Ermittlern den ungefähren Standort des Geräts und damit auch des Betroffenen.

Nicht mehr öffentlich verraten will die Regierung erstmals auch, wie viele Funkzellenabfragen die Zollfahnder durchführten. 2019 nutzten diese das Verfahren, bei dem Verbindungsdaten aller in eine bestimmte Funkzelle zu einem bestimmten Zeitpunkt eingeloggter Handy-Nutzer gespeichert und gerastert werden, in 44 Fällen. Hunko kritisierte diese erweiterte Heimlichtuerei „aufs Schärfste“. Weil damit das parlamentarische Fragerecht ausgehöhlt werde, habe er beim BMI Beschwerde eingereicht. Handys seien generell zum Telefonieren da, „nicht um sie zunehmend als Ortungswanzen zu missbrauchen“.

Die Bundespolizei fragte 2020 in 77 Fällen Providerdaten mithilfe von Funkzellenauswertungen ab. Im Vorjahr hatte sie davon 96-mal Gebrauch gemacht, um nachträglich alle Mobiltelefone in der Umgebung von Tatorten festzustellen. Das BKA gebrauchte das Instrument im vorigen Jahr in einem Fall, 2019 waren es drei Fälle gewesen. Der Generalbundesanwalt führte in vier Fällen insgesamt fünf Funkzellenauswertungen durch, wobei er sich der Amtshilfe von Landeskriminalämtern in Bayern, Baden-Württemberg und Nordrhein-Westfalen bediente. Das BMI wollte oder konnte nicht die Zahl der Maßnahmen benennen, „die wesentlich zur Aufklärung der jeweiligen Straftat beigetragen haben“.

IMSI-Catcher brachte die Bundespolizei in 28, das BKA in vier Fällen in Stellung, um den Standort eines aktiv geschalteten Mobiltelefons und die Geräte- oder Kartennummer zu ermitteln. In Verfahren des Generalbundesanwalts wurden im ersten Halbjahr 2020 in 14 sowie im zweiten in 13 Fällen derlei Anlagen eingesetzt. IMSI-Catcher senden mit einem stärkeren Signal als Basisstationen der offiziellen Netzbetreiber, sodass sich Handys dort einwählen und so überwacht werden können.

Das Werkzeug liefert dem BMI zufolge wesentliche Ausgangspunkte für weitere Ermittlungsmaßnahmen, durch die Sachverhalte inhaltlich aufgeklärt werden können. Die Bundesregierung habe 2020 auch eine Ausfuhrgenehmigung für einen IMSI-Catcher erteilt und zwar nach Ungarn. Über das belieferte Unternehmen könne man keine Angaben machen, um Betriebs- und Geschäftsgeheimnisse zu wahren. Keine öffentliche Auskunft gibt die Exekutive darüber, wie viele solche Abhöranlagen Bundesbehörden im Regierungsviertel aufgespürt haben.

Jenseits der Handy-Überwachung befassen sich mit der „Internetaufklärung“ beim BfV „alle Fachabteilungen“. Nähere Auskünfte zur Aufgabenverteilung und zu Personalstärken könnten zum Schutz der Arbeitsweise des Geheimdienstes nicht gegeben werden. Innerhalb des BKAs seien die Abteilungen Polizeilicher Staatsschutz und Islamistisch motivierter Terrorismus/Extremismus damit beschäftigt, Online-Inhalte koordiniert auszuwerten. Das Bundesverteidigungsministerium unternehme in den Abteilungen Strategie und Einsatz offene Recherchen (Open Source Intelligence) zu „Nachrichten, gemeldeten Vorgängen und Ereignissen“ (Krempl, Überwachung: Bundespolizei verschickte 2020 über 100.000 stille SMS, www.heise.de 06.02.2021, Kurzlink: https://heise.de/-5047855).

Bund

Bär-Büroleiterin Reuss wechselt zu Facebook

Die Büroleiterin von Digitalministerin Dorothee Bär (CSU) Julia Reuss wechselte Ende Februar 2021 vom Kanzleramt zum US-Konzern Facebook. Dort ist sie für den Bereich Zentraleuropa zuständig. Die promovierte Politikwis-

senschaftlerin ist seit zwei Jahren die Freundin von Verkehrsminister Andreas Scheuer (CSU). Reuss soll die Zusammenarbeit zwischen dem US-Konzern und politischen Entscheidungsträgern sowie zivilgesellschaftlichen Akteuren vorantreiben. Ihr offizieller Titel: Public Policy Director, Central Europe.

Nur knapp zwei Jahre war Reuss für Bär tätig. Zuvor leitete sie im Bundesverkehrsministerium die Stabsstelle Urbane Mobilität und wurde dort nach nur drei Monaten im Dienst verbeamtet (November 2018). Diesen Status verliert die 37-Jährige nun durch den Wechsel in die Wirtschaft. Zuvor hatte Julia Reuss schon einmal einen Berufswechsel vollzogen, dem ein gewisses Geschmäckle nachgeht: 2012 war sie persönliche Referentin des damaligen Bundesverkehrsministers Peter Ramsauer (CSU). Zum Jahreswechsel übernahm sie dann einen deutlich höher dotierten Posten bei der Deutschen Bahn AG, deren Eigentümer der Bund ist. Das Verkehrsunternehmen hat zahlreiche Berührungspunkte mit der Arbeit einer Referentin im entsprechenden Ministerium.

Die Opposition reagierte pikiert auf die Personalie Reuss, so. z.B. Jan Korte, Parlamentarischer Geschäftsführer der Linken im Bundestag: „Es gibt aus gutem Grund Anzeige- und Genehmigungspflichten auch für Beamte in der Bundesregierung. Natürlich ist es problematisch, wenn die Büroleitung der Beauftragten der Bundesregierung für Digitalisierung im Kanzleramt direkt in die Lobby-Abteilung von Facebook wechselt." Dabei geht es dem Politiker, der sich jahrelang für ein Lobbyregister im Bundestag eingesetzt hatte (s.u.), vor allem um die Haltung der Bundesregierung zu Transparenz. Wenn die Digital-Staatsministerin zulasse, dass „besonderes Wissen aus der Arbeit der Bundesregierung in der Wirtschaft versilbert wird, schadet sie dem Vertrauen in demokratische Institutionen".

Von solchen Klüngel-Vorwürfen wollte man bei Staatsministerin Dorothee Bär nichts wissen. Reuss habe sich eigenverantwortlich für einen Wechsel in die Privatwirtschaft entschieden, so ihr Büro: „Mit Kenntnis über den neuen Arbeitgeber hat Staatsministerin Bär unverzüglich die Übergabe der operativen Tätigkeiten von Frau Dr. Reuss veranlasst." Dort versicherte man außerdem, dass zu den Aufgaben der ehemaligen Büroleiterin „nicht die inhaltliche Betreuung von Themen, die ihren neuen Arbeitgeber betreffen" gehörte (Rebhan, Aus dem Digitalministerium zu Facebook: Scheuers Freundin macht Karriere, www.businessinsider.de 10.02.2021).

Bund

Gesetz zu Lobbyregister verspricht mehr Transparenz

Union und SPD haben sich nach langem Streit auf Regeln für Lobbyisten verständigt, die bei der Bundesregierung und im Parlament ihre Interessen vertreten. Künftig sollen diese verpflichtet werden, sich in ein Lobbyregister einzutragen und ihre Auftraggeber sowie finanziellen Aufwendungen offenzulegen. Die Einigung erfolgte kurz nach dem Bekanntwerden einer Lobby-Affäre um den stellvertretenden Unionsfraktionsvorsitzenden Georg Nüßlein. Gegen den CSU-Politiker laufen Ermittlungen wegen des Anfangsverdachts der Bestechlichkeit, er soll sich bei der Bundesregierung für den Kauf von Schutzmasken eingesetzt und dafür Geld bekommen haben.

Im Sommer 2020 hatte die Lobby-Affäre um den CDU-Abgeordneten Philipp Amthor Bewegung in die seit Jahren stockenden Bemühungen um verbindliche Regeln für Interessenvertreter gebracht. Im August legten Union und SPD einen Gesetzentwurf für ein Lobbyregister vor (DANA 3/2020, 185). Die neuen Regeln sollten aber nur für Lobbyisten gelten, die bei Abgeordneten vorstellig werden, aber nicht für diejenigen, die sich direkt an die Bundesregierung wenden. In ihrer traditionellen Sommerpressekonferenz hatte Bundeskanzlerin Angela Merkel erklärt, damit lege die Regierung schon „eine sehr hohe Transparenz an den Tag". Da aber die meisten Gesetze in den Ministerien und nicht im Parlament entworfen werden, wäre damit ein zentraler Bereich des Lobbyismus im Schatten geblieben. Nach massiver öffentlicher Kritik lenkte die Koalition ein und sagte zu, das Lobbyregister werde für Parlament und Regierung gelten.

Innerhalb der Bundesregierung gab es Einwände: Das Innenministerium unter Führung von Horst Seehofer (CSU) wollte nur Kontakte mit der Führungsebene der Ministerien registrierungspflichtig machen, nicht aber mit den Fachabteilungen. Der Bundesjustizministerin Christine Lambrecht (SPD) gingen die Pläne dagegen nicht weit genug. Sie wollte in dem Entwurf noch den „exekutiven Fußabdruck" unterbringen, der für jedes neue Gesetz dokumentiert, welche Lobbyisten bei der Regierung Einfluss genommen haben. Dieser Streit konnte über Monate nicht ausgeräumt werden.

Am 02.03.2021 morgens verständigten sich die Fraktionschefs Ralph Brinkhaus (CDU) und Rolf Mützenich (SPD) darauf, dass es eine Einigung beim Lobbyregister geben müsse; abends stand der Kompromiss. Die Registrierungspflicht soll künftig nicht nur für Lobbyisten-Kontakte mit Ministern und Staatssekretären, sondern auch mit Abteilungs- und Unterabteilungsleitern gelten. An dieser Stelle gab die Union nach. Dafür verzichtete die SPD am Ende darauf, den exekutiven Fußabdruck durchzusetzen. Den Interessenvertretern wird ein Verhaltenskodex auferlegt. Wer sich nicht registriert oder wer falsche Angaben macht, begeht künftig eine Ordnungswidrigkeit, die mit einem Bußgeld bis zu 50.000 € geahndet werden kann. Im Bundestag saßen Anfang 2021 709 Abgeordnete. Es gab fast 800 Lobbyisten, die über einen Hausausweis für das Parlamentsgebäude verfügten. Insgesamt gibt es mehrere Tausend Lobbyisten in Berlin.

Nach dem Kompromiss erhoben beide Seiten Vorwürfe gegen die jeweils andere, so Mützenich: „Endlich hat die Union eingelenkt, nachdem die jahrelange Blockade auch vor der Öffentlichkeit nicht mehr vertretbar war." Der parlamentarische Geschäftsführer der Unionsfraktion, Patrick Schnieder, warf dagegen der SPD vor, eine Einigung blockiert zu haben: „Die Justizministerin erhob plötzlich Forderungen, die bereits vom Tisch waren." Er betonte, die Einigung stehe nicht in Zusammenhang mit den Vorwürfen gegen Nüßlein. Die Union warte das Ergebnis der Ermittlungen

ab und werde sich dann damit auseinandersetzen, ob es Regelungslücken gebe. „Weder der Fall Nüßlein noch der Fall Amthor haben inhaltlich etwas mit dem Lobbyregister zu tun.“ Hier gehe es vielmehr um das Abgeordnetengesetz und die Verhaltensregeln für Abgeordnete.

FDP, Grüne und Linke bemängelten das Fehlen des exekutiven Fußabdrucks. Der parlamentarische Geschäftsführer der Linken, Jan Korte, kritisierte: „Worauf die Koalition sich nun geeinigt hat, ist ein Lobbyregister light.“ Er bedauerte, dass sich die SPD gegenüber der Union nicht durchgesetzt habe, obwohl bei der Union wegen der Lobby-Affären „die Hütte brennt“. Die parlamentarische Geschäftsführerin der Grünen, Britta Haßelmann, meinte, was CDU/CSU und SPD vorschlagen, sei „unzureichend“. Der Vorsitzende der Organisation Transparency Deutschland, Hartmut Bäumer, nannte das Lobbyregister der großen Koalition „ein Placebo zur Beruhigung der weniger informierten Öffentlichkeit“. Wirkliche Transparenz der Lobbyarbeit werde dieses Gesetz nicht bewirken (von Salzen, Warum sich Union und SPD nach langem Streit auf ein Lobbyregister einigen, www.tagesspiegel.de 03.03.2021; Rossmann, Transparenz per Gesetz SZ 25.03.2021).

Bund

Parlamentarische Offenlegungsregeln werden verschärft

Mitte April 2021, ca. drei Wochen nach der Einigung der großen Koalition auf schärfere Transparenzregeln für Parlamentarier, haben CDU, CSU und SPD ihren Gesetzentwurf für eine Änderung des Abgeordnetengesetzes fertiggestellt, wo es in den Vorbemerkungen heißt: „Das Vertrauen der Bürgerinnen und Bürger ist das Fundament des deutschen Parlamentarismus. Bereits der Verdacht, dass Mitglieder des Deutschen Bundestages ihr Mandat missbrauchen, um eigene monetäre Interessen zu verfolgen, kann das Vertrauen in die Unabhängigkeit der Abgeordneten und die Integrität des Deutschen Bundestages unterlaufen.“

Mit der Änderung des Abgeordnetengesetzes werden die bisherigen Transparenzregeln deutlich verschärft. Die bislang in der Geschäftsordnung des Deutschen Bundestages sowie in deren Ausführungsbestimmungen festgelegten Verhaltensregeln für Abgeordnete werden in einen neuen elften Abschnitt des Gesetzes überführt. So erhalten die Transparenzvorschriften Gesetzesrang und werden übersichtlicher.

Neu ist, dass die Nebeneinkünfte auf Euro und Cent offengelegt werden müssen, sofern sie eine Bagatellgrenze von 1.000 € im Monat oder maximal 3.000 € im Jahr überschreiten. Bislang waren nur Honorare oberhalb von 10.000 € im Jahr veröffentlichungspflichtig. Außerdem mussten Abgeordnete lediglich Stufenwerte für ihre Einkünfte angeben, nicht aber die genauen Beträge. Neu ist auch die Pflicht mittelbare und unmittelbare Beteiligungen an Unternehmen anzugeben, wenn sie einen Anteil von 5% übersteigen. Bislang lag der Schwellenwert bei 25%. Die Interessenvertretung gegenüber anderen Abgeordneten oder der Bundesregierung wird Mitgliedern des Bundestages verboten. Das gilt auch für Beratertätigkeiten, die im Zusammenhang mit dem Mandat stehen.

Abgeordnete sollen keine Spenden mehr annehmen dürfen. Auch Honorare für Vorträge, die im Zusammenhang mit der Abgeordnetentätigkeit stehen, dürfen sie nicht mehr kassieren. Gastgeschenke, die sie im Rahmen ihrer Mandatsausübung bekommen, dürfen Abgeordnete bis zu einem Wert von 200 € behalten. Teurere Geschenke müssen sie dem Präsidenten des Bundestages aushändigen oder können sie gegen Zahlung des Gegenwertes an die Bundeskasse behalten.

Der Gesetzentwurf räumt zudem mit einer von vielen selbstständigen Abgeordneten als ungerecht empfundenen Veröffentlichungspraxis auf: Wer ein Unternehmen betreibt, muss künftig nicht mehr seine Bruttoumsätze veröffentlichen, sondern den Gewinn vor Steuern. Die Zeiten, in denen Landwirte fälschlicherweise als Spitzenverdiener des Parlaments ausgewiesen wurden, dürften damit vorbei sein.

Mit dem Gesetz reagiert die Koalition auf die Lobby- und Maskenaffäre in der Bundestagsfraktion von CDU und CSU, in deren Folge mehrere Parlamentarier ihr Mandat niedergelegt haben. Der SPD-Sprecher im Ausschuss für Wahlprüfung, Immunität und Geschäftsordnung Mathias Bartke erläuterte: „Die Skandale der Vergangenheit haben gezeigt, dass neue Verhaltensregeln für Abgeordnete dringend notwendig sind. Bezogen auf wirtschaftliche Aktivitäten schaffen wir mit dem Gesetz einen weitgehend gläsernen Abgeordneten. Dies gilt insbesondere für die Veröffentlichungspflicht von Nebeneinkommen nach Euro und Cent und die Offenlegungspflicht von Unternehmensbeteiligungen ab 5 Prozent. Parlamentarische Vorgänge werden für Außenstehende künftig deutlich transparenter“ (Niesmann, Das Transparenzgesetz, Kieler Nachrichten 17.04.2021, 5).

Bundesweit

DSGVO-Bußgelder blieben 2020 weitgehend bescheiden

Bei einer Umfrage des Handelsblatts nach Verstößen gegen die Datenschutz-Grundverordnung (DSGVO) bei den Aufsichtsbehörden kam heraus, dass im Jahr 2020 knapp 60% mehr Bußgelder verhängt wurden als im Jahr zuvor. Keine Angaben macht die Aufsicht von Mecklenburg-Vorpommern. Betroffen von Strafen und geringeren Bußgeldern sind vor allem viele kleine und mittlere Unternehmen sowie Soloselbstständige. Die Strafzahlungen beliefen sich bundesweit insgesamt auf 48 Millionen Euro. Den mit Abstand größten Batzen macht das Bußgeld gegen den Modehändler H&M aus, der alleine 35 Mio. € zahlen musste (DANA 4/2020, 253 f.). Die Rekordbuße verhängte der Hamburgische Datenschutzbeauftragte. H&M hatte Mitarbeiter in einem Servicecenter in Nürnberg ausgespäht und private Daten gesammelt – von Urlaubserlebnissen bis zu Krankheitssymptomen.

Es folgt ein Bußgeld in Höhe von 10,4 Millionen Euro, das die niedersächsische Datenschutzbeauftragte gegen Notebooksbilliger.de verhängt hat (DANA 1/2021, 45). Anders als H&M, die kein Rechtsmittel einlegen wollten, um den Fall möglichst schnell zu beenden, wehrt sich den Elektronikartikelanbieter gegen die Vorwürfe unzulässigerweise Mitar-

beiter überwacht zu haben. Die AOK in Baden-Württemberg musste wegen der Nutzung von Daten zu Werbezwecken ohne Einwilligung 1,2 Millionen Euro zahlen (DANA 3/2020, 186).

Es erfolgten auch kleinere Bußgelder, die häufig auf Unwissenheit und Fahrlässigkeit zurückgehen. Ein Anwalt musste 8.000 € zahlen, weil er aufgrund einer Namensgleichheit einen falschen Handwerker als Schuldner beschuldigt hatte. Auch beim Wechsel ins Homeoffice ist es gemäß den Angaben zu Datenpannen gekommen. Die Kontaktdatensammlung zur Nachverfolgung von Infektionsketten hat mehrfach zu Vergehen geführt.

2020 hat es gemäß den Angaben insgesamt 301 Bußen gegeben, 2019 waren es 187. Die meisten Strafen gab es im vergangenen Jahr in Nordrhein-Westfalen (93), gefolgt von Thüringen (40), Sachsen (29) und Niedersachsen (27). Bei den Datenpannen lag dagegen Bayern (5.294) vorn, vor Baden-Württemberg, wo 2.320 gemeldet wurden und Nordrhein-Westfalen (1.775). Der Bundesdatenschutzbeauftragte Ulrich Kelber hat selbst 2020 kein Bußgeld verhängt. Im Jahr zuvor hatte er 1&1 zu einer Strafe von 9,6 Millionen Euro verdonnert, die ein Gericht auf 900.000 Euro herabsenkte (DANA 1/2020, 50, 1/2021, 62) (Weiß, Mehr Bußgelder wegen DSGVO-Verstößen in 2020, www.heise.de 16.02.2021, Kurzlink: https://heise.de/-5056383).

Bundesweit

Eventus-Datenleck bei Corona-Schnelltests

Bei einer Betreiberin von Corona-Schnelltestzentren, der auf die Vermarktung von Verbrauchsgütern spezialisierten Firma Eventus Media International, kam es für Betroffene in verschiedenen Städten, u.a. Berlin, Hamburg und Leipzig, durch eine schlechte Absicherung der Webseite testcenter-corona.de zu einem Datenleck. Betroffen von der Lücke waren am 06.04.2021 über 14.000 Registrierungen mit hinterlegtem Testergebnis und persönlichen Daten wie Name, Anschrift, Geburtsdatum, Telefonnummer und E-Mail-Adresse.

Entdeckt hat das Leck die Hackergruppe Zerforschung, die auch zusammen mit dem Chaos Computer Club (CCC) einer Sicherheitslücke beim Startup 21DX und dessen Dienstleister Medicus Ai auf die Spur gekommen war, über die Informationen von rund 130.000 Getesteten abgerufen werden konnten. Diesmal waren 5.800 Bürger in Leipzig, jeweils rund 3.000 in Berlin und Hamburg, 1.400 in Schwerte sowie 800 in Dortmund betroffen. Statt die eigene Website von Grund auf selbst zu entwickeln, hatte Eventus die betroffene Domain laut den IT-Sicherheitsexperten auf dem weitverbreiteten Open-Source-Blog- und Content-Management-System WordPress aufgesetzt. Das Unternehmen nutzte die dafür vorhandene breite Palette an Erweiterungen für das Buchen von Terminen und Abrufen von Testergebnissen. Der Nutzer muss dafür eine zufällige zehnstellige, alphanumerische Zeichenkette eingeben.

Zum Verhängnis wurde Eventus, dass die Zuständigen für die Testzentren-Homepages einen eigenen Wordpress-Inhaltstypus „registration“ für Schnelltest-Registrierungen anlegten und als Schnittstelle (API) verfügbar machten. Darauf bildeten sie Terminbuchungen und Testzertifikate ab. Die API-Zugriffsmöglichkeit dafür war entgegen üblicher Gepflogenheiten aktiviert, sodass alle Registrierungen auch darüber von außen abrufbar waren. Die Tüftler fanden dabei in der abgefragten Liste sämtliche Abrufcodes für Ergebnisse und die damit verknüpften persönlichen Informationen: „Das ist in etwa so, als würde man sich einen Safe einbauen lassen, aber den Code dann direkt daneben legen.“ Die zehnstelligen Zeichenfolgen hätten sich auf der Testergebnisabfrage-Seite eingeben und die Resultate dann zusammen mit einem informationsreicheren PDF für eine gegenüber Dritten vorzeigbaren Bescheinigung herunterladen lassen. Zudem habe es kein Limit gegeben, wie viele Ergebnisse in einem definierten Zeitraum abrufbar gewesen seien. Eine solche Grenze hätte die Hürde für Angreifer etwas erhöht.

Um möglichst schnell die abrufbaren sensiblen Gesundheitsdaten zu schützen und die Lücke zu schließen, schlugen die Forscher beim Bundesamt für Sicherheit in der Informationstechnik (BSI) Alarm. Dieses habe das Problem anonymisiert an Eventus weitergeleitet. Die Firma habe das Leck noch am selben Tag abgedichtet. Zusätzlich führte sie am nächsten Tag ein weiteres Feld zur Abfrage zusätzlicher Angaben beim Abruf eines Testergebnisses ein. Codes, die vor der Umstellung erstellt worden waren, setzte das Unternehmen zurück und schickte den Betroffenen neue Zugangsdaten.

Ein Eventus-Sprecher räumte ein, dass man die Testcenter einschließlich der damit verbundenen Datenverarbeitungssysteme „mit großer Eile hochgezogen“ habe. Dabei sei zwar eine Zusammenarbeit mit „versierten IT-Spezialisten“ erfolgt, um „die größtmögliche Sicherheit gewährleisten zu können“. Die Firma entschuldigte sich dafür, „dass Hacker trotzdem auf einen Teil der Daten zugreifen konnten“.

Zerforschung zufolge waren drei Tage nach dem Bekanntwerden des Leaks die Kunden noch nicht über die Panne informiert worden. Um solche Vorfälle künftig zu vermeiden, sollten die Datenschutzbehörden „empfindliche Strafen verhängen“. Der Schutz von Gesundheitsdaten dürfe auch in einer Pandemielage nicht auf die leichte Schulter genommen werden, schnelle Handlungsfähigkeit dürfe keine Ausrede sein. Unternehmen müssten ihrer Sorgfaltspflicht vor dem Start eines digitalen Angebots nachkommen (Krempl, Sicherheitslücke: Daten tausender Corona-Getesteter ungesichert im Netz, www.heise.de 09.04.2021, Kurzlink: https://heise.de/-6010505).

Bundesweit

Künast verklagt Facebook wegen Falschzitat

Die Bundestagsabgeordnete Renate Künast (Grüne) hat vor dem Landgericht Frankfurt am Main (LG) Klage gegen Facebook eingereicht, um eine Grundsatzentscheidung zur Löschung von Hasspostings herbeizuführen. Das geht aus einer Unterlassungserklärung hervor, die Künast an die irische Europazentrale von Facebook geschickt hat. Die Bundestagsabgeordnete fordert darin, dass Facebook nicht nur einen einzelnen

Beitrag mit einem ihr fälschlicherweise zugeschriebenen Zitat löscht, sondern auch alle „identischen" und „sinngleichen Inhalte auf der ganzen Plattform".

Sie erklärte: „Ich habe mich lange mit dem Thema beschäftigt und gesehen, welche Wucht mit organisiertem und orchestriertem Rechtsextremismus entwickelt werden kann. Ein Werkzeug ist, Zitat zu erfinden und dann rumzuschicken. Ich möchte für alle Betroffenen erreichen, dass das Vorgehen gegen Falschzitate nicht zu ihrer energiefressenden Lebensaufgabe wird." Sie persönlich habe genug davon, dass Facebook die eigene Verantwortung leugne. „Es kann nicht sein, dass ich als einzelne Betroffene es mir zur Lebensaufgabe machen muss, das gesamte Facebook-Netz abzusuchen, um jede Kopie eines verleumderischen Falschzitats zu suchen, zu melden und dann löschen zu lassen. Ich möchte an dieser Stelle eine Grundsatzentscheidung hinbekommen." Eine solche Entscheidung könne eine grundsätzliche Wirkung darauf haben, wie sich Menschen in dieser Gesellschaft einbringen.

Die Klage vor dem LG wird von der gemeinnützigen Organisation Hate Aid und der Alfred Landecker Foundation unterstützt. Eingereicht wurde die Klage durch die Würzburger Kanzlei von Chan-jo Jun, die bereits mehrfach gegen Facebook klagte. Bei dem Facebook-Beitrag handelt es sich um eine Bild-Text-Kachel, in der neben einem Foto von Künast das folgende Zitat steht, welches frei erfunden ist: „Integration fängt damit an, dass Sie als Deutscher mal Türkisch lernen." Dieses falsche Zitat wurde wiederholt auf Facebook geteilt und führte zu Hasskommentaren gegen die Politikerin. In Fällen von solchen Verleumdungen müssen Betroffene bisher jeden einzelnen Beitrag an Facebook melden, damit er anschließend von Firmenmitarbeitern geprüft wird. Falls der gleiche Beitrag an anderer Stelle im sozialen Netzwerk – zum Beispiel in geschlossenen Gruppen – von anderen Nutzern veröffentlicht wurde, bleibt er dort online.

Hate-Aid-Geschäftsführerin Anna-Lena von Hodenberg sagte, wenn solche Falschinformationen über Privatpersonen teils tausendfach hochgeladen und geteilt würden, könne dies Leben zerstören. Die Beratungsstelle der Organisation arbeite an Dutzenden ähnlichen Fällen.

Facebook hatte sich im aktuellen Fall bereit erklärt, zumindest alle identischen Kopien des umstrittenen Beitrags zu löschen, so ein Sprecher des Konzerns: „Wir haben das von Frau Künast gemeldete falsche Zitat von der deutschen Facebook-Plattform entfernt und Frau Künast darüber informiert, dass wir ebenfalls Schritte einleiten, um identische Inhalte zu identifizieren und zu entfernen."

In der letzten Zeit erleben Menschen noch mehr Hass im Internet als zuvor. Viele der Äußerungen sind rechtswidrig, doch die Betroffenen können ihre Rechte auf Löschung und Strafverfolgung nur schwer durchsetzen. Das liegt, so Künast, an der mangelnden Kooperation von Facebook, Twitter und anderen Plattformbetreibern, die es darauf ankommen ließen, dass die Betroffenen ihre Rechte vor Gericht einklagen. Da es kaum Rechtsprechung gibt und sich die Unternehmen wehren, sind Betroffene gezwungen den Weg durch die Instanzen zu gehen. Das ist aufwändig und teuer; die meisten Betroffenen trauen sich darum nicht. So kommen die Täter mit ihrem Verhalten durch. Meist sind es Frauen, die zum Ziel von Hass im Netz werden, so Anna-Lena von Hodenberg: „Es trifft Kommunalpolitikerinnen, Aktivistinnen und Journalistinnen, die mundtot gemacht werden sollen. Leider ist das erfolgreich." Künast will nicht zulassen, dass die Medienkonzerne diesen Hass weiter befeuern und damit Geschäfte machen: „Die Zukunft der Demokratie wird im Netz entschieden" (Renate Künast verklagt Facebook wegen Falschzitat, www.zeit.de 27.04.2021; Werner, Renate Künast verklagt Facebook, SZ 28.04.2021, 16)

Bundesweit

Datenschutzaufsicht zu Warnungen vor IT-Produkten berechtigt

Ein durch den Arbeitskreis (AK) Grundsatz der Datenschutzkonferenz erstelltes und publik gewordenes vorläufiges Gutachten kommt zu dem Schluss, dass es unter Einhaltung des Gebots der Sachlichkeit und der Richtigkeit rechtens ist, wenn Datenschutzaufsichtsbehörden vor dem Einsatz bestimmter IT-Produkte warnen. In der Vergangenheit waren die deutschen Datenschutzbehörden mit Aussagen zu Produkten eher zurückhaltend. Zuständig für Warnungen vor deren Einsatz waren ihrer Auffassung nach eher Verbraucherschutzverbände oder, wenn es um die IT-Sicherheit ging, das Bundesamt für Sicherheit in der Informationstechnik.

Der Bedarf von Unternehmen und Verwaltungen nach Videokonferenz-Diensten und Collaboration-Tools während der Corona-Pandemie führte zu steigenden Beratungsanfragen. Zunehmend äußerten sich Datenschützer zu solchen Tools und sprachen Empfehlungen oder Warnungen aus, meist nach Kriterien der Datenschutzkonformität wie Verschlüsselung, Verarbeitung und Übertragung personenbezogener Daten, Privacy-Einstellungen der Tools usw. Prominente Beispiele sind die Warnung vor dem Einsatz von Zoom durch den Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI) Stefan Brink, die er nach Nachbesserungen durch Zoom wieder zurücknahm, oder die ständig aktualisierte Liste der gängigsten Videokonferenz-Tools mit Ampelwertungen der Berliner Beauftragten für den Datenschutz und die Informationsfreiheit (BlnBDI) Maja Smoltczyk.

Da solche Warnungen erhebliche Auswirkungen auf Unternehmen haben können, etwa Umsatzeinbußen oder eine schlechte Reputation, war umstritten, ob Aufsichtsbehörden hierzu befugt sind. In einer Zwischenkonferenz beschlossen die Datenschutzbehörden des Bundes und der Länder die Rechtmäßigkeit solcher Warnungen zu überprüfen und beauftragten den AK Grundsatz, „die Rahmenbedingungen aufsichtsbehördlicher Produktwarnungen, insbesondere Rechtsgrundlagen, Anforderungen an Beweiserhebung und Verfahren sowie Haftungsfragen zu analysieren und der Datenschutzkonferenz möglichst bis zur 100. Sitzung der Konferenz der unabhängigen

Datenschutzaufsichtsbehörden des Bundes und der Länder zu berichten“.

Dieses (vorläufige) Gutachten liegt nach einer Anfrage gemäß dem Informationsfreiheitsgesetz vor. Eine Rechtsgrundlage für „aufsichtliche Produktwarnungen“ ist nach Auffassung des AK Grundsatz durch die DSGVO sowie durch manche Landesdatenschutzgesetze grundsätzlich gegeben. Sie müssen inhaltliche Kriterien erfüllen: Der zugrundeliegende Sachverhalt muss „sorgsam aufgeklärt und richtig wiedergegeben sein“. Die Richtigkeit bedeutet in diesem Zusammenhang auch, dass bei Software jedes Update erneut zu überprüfen ist beziehungsweise die Warnung nur für die entsprechenden Versionen ausgesprochen wird.

Des Weiteren muss die Warnung sich ausschließlich auf sachliche Gründe beziehen, sachfremde Erwägungen sind ebenso unzulässig wie eine unsachliche oder herabsetzende Darstellung. Vor Aussprechen einer Warnung ist zu prüfen, ob dieses Vorgehen angemessen ist oder vielleicht „mildere Mittel“ ebenfalls zur Vermeidung von Datenschutzverletzungen führen können – beispielsweise eine Abstimmung mit dem Hersteller, der den Mangel zeitnah abstellen könnte. Halten die Datenschutzbehörden diese Voraussetzungen für eine Produktwarnung nicht ein, kann das zu Unterlassungsansprüchen führen oder gar eine Haftung auslösen.

Diese Bedingungen sind eine Herausforderung für die Aufsichtsbehörden, denn es dürfte schwierig sein alle Produkte umfassend zu beurteilen und sich nicht nur einige Punkte herauszugreifen. Weitere Schwierigkeiten bestehen darin, dass die verschiedenen Datenschutzbehörden nicht zwingend dieselbe Rechtsauffassung haben, zum Beispiel was die Datenübermittlung in Drittländer anbelangt. Was für den einen rechtswidrig ist, ist für die andere rechtskonform und nicht zu beanstanden. Da sich aus diesem Zwischenstand weitere Fragen ergeben haben, will das Gutachten nicht abschließend sein (Roos, Datenschutzaufsichtsbehörden dürfen vor IT-Produkten warnen, www.heise.de 08.04.2021, Kurzlink: https://heise.de/-6009097).

Baden-Württemberg

Bußgeld gegen den VfB Stuttgart wegen Datenmissbrauch

Am 10.03.2021 hat der Landesdatenschutzbeauftragte von Baden-Württemberg (LfDI) Stefan Brink mit einer Bußgeldfestlegung in Höhe von 300.000 € den September 2020 bekannt gewordenen Datenskandal beim VfB Stuttgart abgeschlossen. Geahndet wurde die „fahrlässige Verletzung der datenschutzrechtlichen Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO“. Der Verein verpflichtet sich in Abstimmung mit der Behörde zudem zu einer kostenträchtigen Umstrukturierung seines Datenschutzmanagements sowie zu weiteren Maßnahmen. So will man insbesondere junge Menschen für Datenschutzanliegen sensibilisieren.

Hierzu will der Bundesligist die Initiative „Datenschutz geht zur Schule“ (siehe Seite 85) fördern. Realisiert werden soll das durch Unterstützung bei der Öffentlichkeitsarbeit für regionale Schul-Aktionstage und im Rahmen kind- und jugendgerechter Videos zur Sensibilisierung für datenschutzrelevante Themen. Zudem will der VfB zum Thema „Datenschutz bei Jugendlichen“ Schulungen für seine Nachwuchsmannschaften von der U10 bis zur U21 konzipieren.

Hintergrund des Verfahrens ist, dass im Jahr 2017 rund 100.000 Datensätze, unter anderen von Mitgliedern, an Dritte weitergegeben und für Marketingmaßnahmen missbraucht wurden, als es um die Zustimmung der Mitglieder bei der Entscheidung ging, ob der Bundesligist seine Fußballsparte in eine Aktiengesellschaft (AG) ausgliedern soll, was letztlich mit einer Mehrheit von 84% bestätigt wurde. VfB-Präsident Claus Vogt hatte nach Bekanntwerden der Datenaffäre die Kanzlei Esecon mit der Untersuchung des Vorgangs beauftragt, die in ihrem Abschlussbericht zu dem Ergebnis kam, dass der Verein die Daten an den externen Dienstleister weitergegeben hat, ohne die Mitglieder darüber zu informieren. Dies sei ein „Täuschungsversuch“ und „damit ein Vertrauensbruch“ gewesen. Es sei „sehr wahrscheinlich“, dass die Daten für „Guerilla-Marketing“ benutzt worden seien, um subtil Einfluss zu nehmen. Ziel sei es gewesen die Anhänger 2017 im Vorfeld der Mitgliederversammlung von der Ausgliederung des Profifußballs in eine Aktiengesellschaft zu überzeugen. Die Aufklärungsarbeit sei von mehreren Funktionsträgern im Verein behindert worden. Die Zuordnung der Verantwortlichkeit war dadurch erschwert worden, dass die relevante Mail auf dem VfB-Server gelöscht worden war.

Über die rechtliche Bewertung der Esecon-Ergebnisse hatte es beim VfB einen heftigen Streit gegeben. Vogt meinte zunächst, man müsse das „erst einmal intern klären. Es gibt unterschiedliche Anschauungen darüber, wer die rechtliche Bewertung vornehmen soll“. Vogt hatte dann am 04.02.2021 die Stuttgarter Staatsanwaltschaft eingeschaltet, da „der Verdacht eines Geheimnisverrats (…) im Raume steht“. Es gebe „das Ziel und die Absicht“, ihn persönlich zu beschädigen: „Dieser Schritt war nötig geworden, um falschen Gerüchten entgegenzuwirken.“ Nach Erlass des Bußgelds erklärte Vogt: „Hinter uns liegen harte Monate; sie waren auch schmerzhaft. Wir bitten um Entschuldigung für das, was beim VfB passiert ist.“ Der Vorstandschef der gegründeten AG, Thomas Hitzelsberger, der zum Zeitpunkt des Datenmissbrauchs ebenso wie Vogt noch nicht im Amt war, erklärte auch, der Vorgang sei nun abgeschlossen. Schon die Aufklärung der Affäre habe sowohl den eingetragenen Verein als auch die AG jeweils einen sechsstelligen Betrag gekostet. Vogt und Hitzlsberger hatten sich zuletzt einen heftigen Machtkampf geliefert, wollen künftig aber wieder „vernünftig“ zusammenarbeiten.

LfDI Stefan Brink resümierte: „Auch wenn wir mit Blick auf Verjährungsvorschriften nicht alle öffentlich diskutierten Vorgänge vollständig untersuchen konnten, ist doch das jetzt einvernehmlich gefundene Ergebnis überzeugend: Neben dem spürbaren Bußgeld sorgt der VfB für erhebliche organisatorische und technische Verbesserungen in Sachen Datenschutz. Zudem planen die Verantwortlichen erfreulicherweise künftig ein Engagement bei der Aufklärung über Datenschutzanliegen, mit dem vor allem junge Menschen angesprochen

werden sollen." Ende Februar 2021 hat der VfB personelle Konsequenzen gezogen und die leitenden Mitarbeiter Uwe Fischer und Oliver Scharf, die ehemaligen Leiter Marketing und Kommunikation, freigestellt. Im Vorfeld dieser Maßnahme wurden zudem die Vorstände Stefan Heim (Finanzen) und Jochen Röttgermann abberufen (VfB bleibt eine AG, SZ 16.03.2021, 23; Maisel, Stefan Brink setzt Strafmaß für Bundesligisten fest, www.stuttgarter-nachrichten.de 10.03.2021, Ruf, Von der Affäre zur Welle, SZ 27./28.02.2021, 42, „Vertrauensbruch" und „Täuschungsversuch" - Datenschutz-Skandal beim VfB Stuttgart, www.rtl.de 05.02.2021).

Baden-Württemberg

LfDI kritisierte Hochschul-Prüfungssoftware

Der Landesbeauftragte für Datenschutz und Informationsfreiheit von Baden-Württemberg (LfDI) Stefan Brink bewertet eine bei Online-Prüfungen eingesetzte Überwachungssoftware als „hochproblematisch". Die von einigen Hochschulen des Landes in der Corona-Zeit eingesetzte Überwachungssoftware sei „jenseits dessen, was wir als Datenschützer für vertretbar halten".

Studentinnen und Studenten müssen dabei eine „Fernaufsichts-Plattform" auf ihren Rechner spielen, um an einer Prüfung von zuhause teilnehmen zu können. Während des Examens müssten sie dann Kamera und Mikrofon anlassen und dürften ihren Platz vor dem Rechner nicht verlassen. Brink: „Man möchte an der Mimik erkennen, ob jemand betrügt. Das halten wir für Hokuspokus. Das sind massive Eingriffe in die Freiheit der Studentinnen und Studenten." Die Entscheidung über den Einsatz erfolgt häufig durch die Fakultäten. Mit der Software würden Geräte auch „durchforstet", ob sich Hilfsmittel darauf befinden. „Da haben wir eine ganze Reihe von Hinweisen und Beschwerden".

Es gebe einen gesetzlichen Rahmen des Forschungsministeriums für Online-Prüfungen: „Die Hochschulen füllen diesen Rahmen sehr unterschiedlich aus." Brink will demnächst Gespräche mit dem Haus von Wissenschaftsministerin Theresia Bauer (Grüne) führen, um zu klären: „Wo sind die roten Linien und wo werden sie überschritten?" (Datenschützer beanstandet Überwachungssoftware bei Online-Hochschulprüfungen, www.heise.de 08.02.2021, Kurzlink: https://heise.de/-5048988).

Berlin

Zalando ändert auf Druck seine „360-Grad-Überwachung"

Die Behörde der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) veranlasste den Mode-Online-Händler Zalando zu weitreichenden Änderungen an einer seit Jahren im Einsatz befindlichen Software, mit der Beschäftigte bewertet wurden und die von Wissenschaftlern und Beschäftigten kritisiert wurde, weil sie Überwachung, Leistungsdruck und Stress erzeugt. Ende 2019 wurde das System einer „360-Grad-Überwachung" Gegenstand der öffentlichen Kritik. Bei Zalando beurteilen Vorgesetzte und Mitarbeiter umfassend Stärken und Schwächen von den ca. 5.000 Kollegen, was sich auf Gehalt, Jobsicherheit und die Personalakte auswirkt.

Die Berliner Datenschützer erklärten das System nicht grundsätzlich für unzulässig, sehen aber Gefahren: „Eine beschäftigte Person muss im Zweifel nicht nur bei Begegnungen mit Chefin oder Chef jederzeit damit rechnen, dass ihr Verhalten das nächste Zeugnis beeinflusst, sondern auch bei jeder Begegnung mit einer anderen Person des Unternehmens." Um der Überwachung des Personals entgegenzuwirken, darf ein Mitarbeiter nun nur noch von drei anderen bewertet werden. Zuvor waren es acht Personen gewesen. Die oder der Bewertete muss einverstanden sein, wer sie oder ihn bewertet, und darf im Zweifel ein Veto einlegen. Die Bewertungsdaten dürfen nicht mehr zeitlich unbegrenzt aufbewahrt werden, sondern dürfen, abgesehen vom Endergebnis, das in die Personalakte übernommen werden darf, nur kurz gespeichert werden.

Um mehr Transparenz zu schaffen, erhalten die Beschäftigten ein Auskunftsrecht. Dagegen war von Zalando vorgebracht worden, dass dies Auswirkungen auf das Persönlichkeitsrecht der Bewertenden hat. Die Auskunft wird nun erst nach Abschluss des Bewertungszyklus erteilt. Die Auskunft über untergeordnete Personen muss nicht erteilt werden, da dies diese davon abhalten könnte, künftig ehrliche Bewertungen abzugeben. Ohne besondere Gründe angeben zu müssen, dürfen sie in ihre Personalakte Einblick erhalten, soweit umsetzbar direkt am Computer per Passworteingabe im automatisierten Verfahren.

Zalando kam den Forderungen der BlnBDI Ende 2020 nach. Das Unternehmen soll sich dabei – im Vergleich zu anderen Firmen – kooperativ gezeigt haben. Die Personalsoftware Zonar, deren Name inzwischen geändert wurde, erlaubte stichprobenartige Auswertungen. Abgeschafft wurde eine Punkteskala, in der Mitarbeiter zu bestimmten Aspekten positive und negative Bewertungen abzugeben hatten.

Zuvor hatte Europas größter Online-Modehändler das System verteidigt. Es sei „gelebte Feedback-Kultur" und fairer als ein System, in dem allein der jeweilige Chef entscheidet, ob jemand befördert wird oder mehr Gehalt erhält: „Jetzt fließt ein, wie Kollegen, firmeninterne Kunden und Führungskräfte über einen denken".

People-Analytics-Instrumente sind in der Praxis schon weit verbreitet. Notwendig ist bei deren Einsatz, dass Sorgfaltspflichten gegenüber den Beschäftigten eingehalten werden und kein Vertrauen zerstört wird. Negativschlagzeilen wegen einer übermäßigen Mitarbeiterkontrolle trafen neben dem Onlinehändler Amazon auch den französischen Caterer Sodexo.

Bei Zalando existiert das Feedback-System nun zwar weiter, jedoch mit weitreichenden Änderungen. Philipp Staab von der Humboldt-Universität, der die Personalsoftware in einer zweijährigen Studie für die Hans-Böckler-Stiftung untersuchte, bewertete die Vorgaben der Berliner Datenschützer: „Die Behörde hat der Überwachungssoftware ziemlich den Zahn gezogen". Im Tätigkeitsbericht der BlnBDI heißt es: „Einschätzungen von Kolleginnen und Kollegen dürfen in die Bewertung der Arbeitsleistung von Beschäftigten

einfließen, wenn Ablauf und Inhalt den Betroffenen transparent gemacht wird, personenbezogene Daten nur im erforderlichen Umfang erhoben und gespeichert werden und ein dauerhafter Überwachungsdruck vermieden wird." Die Einschränkungen in Sachen Transparenz und Speicherdauer erfolgten bei Zalando erst nach Kritik und Datenschutzkontrolle. Soziologe Staab begrüßt, dass die Daten kürzer gespeichert werden sollen. Zuvor hatten Beschäftigte berichtet, dass Zalando zwar zugesichert habe, Bewertungsdaten rasch zu löschen; die Mitarbeiter hätten diese Daten dann trotzdem noch ein Jahr später gesehen.

Die BlnBDI machte Vorgaben, verhängte aber kein Bußgeld. Staab meint, dass andere Unternehmen mehr aufhorchen würden, wenn Zalando sanktioniert worden wäre: „Offenbar sind solche Vorkommnisse, die sich an der Grenze des Zulässigen bewegen, nur im Einzelfall prüfbar. Und dann dauert so eine Prüfung gut ein Jahr. Das ist ein dramatischer Befund für die Rechte der Arbeitnehmer." Daraus folge, dass es starke Betriebsräte brauche, um Missständen frühzeitig zu begegnen. Gerade bei Dienstleistern und in der Startup-Ökonomie gebe es aber sehr schwache Mitbestimmungsstrukturen. Staab hält deshalb eine politische Debatte über ein spezielles Datenschutzrecht für Beschäftigte für notwendig (Hagelüken/Kläsgen, „Permanenter Überwachungsdruck", SZ 09.04.2021, 15; BlnBDI, Jahresbericht 2020, Kap. 8.1).

Berlin

Datenschutzabmahnung wegen Teslas Wächter-Modus

Ein Tesla-Besitzer hat gemäß einem Video-Bericht der Elektroauto-Vermietung nextmove Post von der Beauftragten des Landes für Datenschutz und Informationsfreiheit bekommen. Darin teilte sie mit, dass ihre Behörde vom Ordnungsamt über seinen Einsatz des Tesla-Wächters informiert worden sei und dass ein dauerhafter anlassloser Betrieb der Kameras „jedenfalls datenschutzrechtlich unzulässig" sei. Tesla bietet auf Grundlage der ohnehin vorhandenen Autopilot-Kameras für alle seine Elektroautos seit einiger Zeit einen sog. Wächter-Modus an, bei dem die Kameras im Stehen weiterlaufen. Wenn etwas dem Tesla sehr nahe kommt oder er erschüttert wird, werden ihre Rundum-Bilder aufgezeichnet. Ein Bußgeld kommt demnach auf den Tesla-Besitzer derzeit nicht zu. Die Datenschutzbehörde ließ ihn wissen, sie gehe sicher davon aus, dass er den Wächter-Modus künftig nur noch dort einsetzen werde, wo keine „unbeteiligten Passanten" aufgenommen werden können.

Dass Teslas Wächter oder auch Dashcams generell mit dem deutschen Recht ihre Schwierigkeiten haben, hatten Datenschützer schon zuvor betont (DANA 4/2020, 227 ff.). Im September 2020 berichtete das TV-Magazin Kontraste über das Thema und zitierte den Datenschutzbeauftragten von Baden-Württemberg dazu, dem zufolge eine „ständige" Aufzeichnung des Verkehrsgeschehens unzulässig ist. Im gleichen Monat bekam Tesla auch wegen der Kameras den deutschen Big Brother Award. Neu ist, dass eine deutsche Behörde konkret einen Tesla-Besitzer angeschrieben und auf die nach ihrer Einschätzung unzulässige Wächter-Nutzung hingewiesen hat.

Um zu erkennen, dass der Tesla-Wächter aktiviert ist, muss man sich dem Auto nähern – dann erscheint ein großer Hinweis mit Auge auf dem Bildschirm im Auto. Von da an werden auch die letzten Minuten der Video-Bilder nicht mehr wie sonst überschrieben, sondern als Wächter-Ereignisse gespeichert, die man sich später ansehen kann. Auf diese Weise wurden angeblich schon mehrere absichtliche oder versehentliche Zerstörungen an Teslas und anderen Autos in deren Umfeld aufgeklärt. Gemäß der Berliner Datenschutzbehörde sind die „schutzwürdigen Interessen" aller anderen Personen im Kamera-Blickfeld höher zu werten als der Wunsch des Tesla-Fahrers nach Video-Sicherheit beim Parken. Weil er keinen Bußgeld-Bescheid bekommen hat, dürfte es vorerst keine gerichtliche Entscheidung über die Kamera-Frage bei Tesla geben. Es wird darüber spekuliert, dass Ordnungsamt-Personal in Zukunft Schulungen für das Erkennen des Wächter-Modus bekommen könnten (Bericht: Tesla-Besitzer wegen Wächter-Modus von Berliner Datenschutz-Behörde verwarnt, teslamag.de 07.03.2021)

Berlin

Zoo-Jahreskarten mit Gesichtserkennung

Der Zoo Berlin will ein System zur Gesichtserkennung einführen, das den Einlass von Personen mit Jahreskarten erleichtern soll. Der Plan, ab dem 20.04.2021 biometrische Daten von den Betreffenden zu erfassen, sorgte in der Berliner Politik für erheblichen Unmut und führte zu datenschutzrechtlichen Zweifeln. Berlins Datenschutzbeauftragte Maja Smoltczyk war nicht vorab über das Vorhaben informiert worden. Nach der Kenntnisnahme wurde dort eine Prüfung eingeleitet und dem Zoo ein Fragenkatalog zugesendet. Smoltczyk erklärte, die automatisierte Erkennung biometrischer Daten sei „nur in Ausnahmefällen" zulässig. Es sei fraglich, „ob diese hier wirklich erforderlich ist und nicht ein milderes Mittel zur Verfügung steht".

Für den Zoo Berlin ist das Projekt Teil seiner Bemühungen um Digitalisierung der Abläufe und um Modernisierung des Einlasses. Bisher müsse bei den Jahreskarten von Hand kontrolliert werden, ob das Foto auf dem Ticket mit der Person übereinstimmt. Das wolle man mit Technik der Paderborner Firma HKS beschleunigen, die sich auf Einlass- und Kassensysteme spezialisiert hat. Spezielle Kameras an einer neuen Drehkreuzanlage am „Löwentor"-Eingang sollen dann beim erstmaligen Besuch Gesichtsmerkmale der Jahreskarteninhaber registrieren und der jeweiligen Karte zuordnen. Bei folgenden Besuchen solle dann ein automatischer Abgleich erfolgen.

Die Nutzung sei, so der Zoo, komplett freiwillig. Die Einführung des neuen Systems erfolge „in enger Abstimmung mit der Datenschutzbeauftragten" des Zoos. Wer seine Daten nicht erfasst haben wolle, könne sich auch weiter wie gewohnt am Einlass kontrollieren lassen. Die Inhaberinnen und Inhaber der Jahreskarten wurden postalisch angeschrieben und informiert. Allerdings weisen die Schrei-

ben nicht explizit darauf hin, dass die Teilnahme freiwillig ist.

Berliner Politiker der rot-rot-grünen Koalition stehen der Sache mit großer Ablehnung gegenüber, so z.B. Sven Kohlmeier, Sprecher der Berliner SPD-Fraktion für Rechts- und Netzpolitik: „Eine Software zur Gesichtserkennung einzuführen, wäre wohl das Letzte gewesen, was mir eingefallen wäre, wenn es um einen beschleunigten Einlass in den Zoo geht". Sven Schüsselburg von der Linkspartei erklärte: „Das geht gar nicht. Zweck und Mittel stehen in keinem Verhältnis." Zoo-Chef Andreas Knieriem musste dem Abgeordnetenhaus in einer Sitzung des Ausschusses für Datenschutz Rede und Antwort stehen.

Der Zeitpunkt das datenschutzkritische System einzuführen war ungünstig gewählt. Erst einen Monat zuvor musste der Berliner Zoo mitteilen, dass ein schweres Datenleck bei einem niederländischen Ticketdienstleister auch Daten seiner Gäste kompromittierte. Zusammen mit dem Berliner Tierpark seien Datensätze zu 400.000 Gästen geleakt (Kannenberg, Zoo Berlin: Streit um Gesichtserkennung für Jahreskartenbesitzer, www.heise.de 09.04.2021, Kurzlink: https://heise.de/-6010595).

Berlin

Grundbuchauskünfte über Minister Spahn im Streit

Am 24.02.2021 stand der Bundesgesundheitsminister Jens Spahn im Bundestag Rede und Antwort zur Pandemie. Praktisch zeitgleich stand in der Bundespressekonferenz der Privatmann Jens Spahn zur Debatte, wobei sein Ministeriumssprecher Hanno Kautz klarstellte: „Das ist eine Privatangelegenheit des Ministers. Ich sitze hier nicht, um die privaten Angelegenheiten des Ministers zu besprechen." Zuvor hatten Zeitungen berichtet, Spahn lasse über seinen Anwalt „offenbar Journalisten unter anderem von Spiegel, Bild, Stern und Tagesspiegel über deren Recherche zu seinen Immobiliengeschäften in Berlin ausforschen", wie sich aus einem Schreiben von Spahns Anwälten an das Amtsgericht im Berliner Bezirk Schöneberg vom Dezember 2020 ergäbe.

Hintergrund ist der Kauf einer Wohnung in Schöneberg durch Spahn, die dem ehemaligen Pharma-Manager Markus Leyck Dieken gehörte. Spahn hatte den Manager Dieken später mit der Geschäftsführung der Gematik GmbH betraut. Die Gematik ist zu mehr als 50% im Besitz des Bundes und soll die Digitalisierung im Gesundheitswesen vorantreiben. Sprecher Kautz erklärte: „Es gibt da keinen Zusammenhang." Spahn habe die Wohnung im August 2017 gekauft, im März darauf sei er erst Gesundheitsminister geworden. Ein Jahr später dann habe sich der Bund an der Firma Gematik beteiligt, im Juli 2019 sei Dieken zum Geschäftsführer berufen worden. Kautz: „Da liegen zwei Jahre dazwischen."

Dennoch reagierte Spahn offenbar äußerst empfindlich auf Nachforschungen von Journalisten beim Grundbuchamt, das zum Amtsgericht gehört. Seine Anwälte forderten das Amtsgericht auf, den gesamten Schriftverkehr mit der Zeitung und „sämtliche etwaige weitere Presseschreiben" mitsamt den Antworten des Grundbuchamtes herauszugeben. Zudem hat Spahn offenbar die Namen all der Journalisten wissen wollen, die sich nach seinen Immobiliengeschäften erkundigt hatten: „Um wen handelt es sich?"

Kautz erklärte, weshalb Spahn seinerseits Nachforschungen anstellen ließ: „Er hat als Privatmann sein Recht gegenüber dem Grundbuchamt wahrgenommen. Eine Einsichtnahme in das Grundbuch erforderte ein berechtigtes Interesse." Tatsächlich haben Pressevertreter das Recht, Informationen bei Grundbuchämtern über die Besitzverhältnisse fremder Immobilien einzuholen, wenn es daran ein übergeordnetes „berechtigtes" Interesse gibt. Im Umfeld von Spahn heißt es, dass einige der Anfragen zu seinen Immobilien ohne jegliche weitere Erklärung gestellt worden seien. Spahn wolle sich das nicht bieten lassen und fordere nur sein Recht auf den Schutz seiner Daten als Privatperson ein. Kautz: „Das Grundbuchamt hat in diesem Fall sowohl gegen die Grundbuchordnung als auch gegen die EU-Datenschutzverordnung verstoßen."

Die Grundbuchämter dürfen grundsätzlich Auskünfte über journalistische Nachfragen geben. Im Jahr 2000 hat das Bundesverfassungsgericht (BVerfG) geurteilt, dass die Behörden dabei umsichtig sein sollten. Dies bezog sich aber auf Recherchen im kriminellen Milieu, bei dem es Versuche geben könnte, Journalisten einzuschüchtern.

Zuvor schon hatten Spahn und sein Ehemann im Sommer 2020 mit Journalisten Probleme gehabt, als die beiden eine Villa im Berliner Bezirk Dahlem gekauft hatten. Pressevertreter hatten sich daraufhin mehrfach beim Grundbuchamt nach dem Kaufpreis erkundigt und dies u.a. mit Spahns Aussage begründet: „Hartz IV bedeutet keine Armut." Obwohl das Grundbuchamt den Betrag daraufhin nannte, ging das Ehepaar gegen genauere Angaben zum Wert der „Millionenvilla" mit Unterlassungsklagen vor. Darin wurde das Paar bestätigt: Das Hamburger Landgericht urteilte, dass der Kaufpreis „rechtswidrig durch ein Durchstechen" an die Öffentlichkeit gekommen sei. Die Summe habe nicht genannt werden dürfen. Der beklagte „Tagesspiegel" hat gegen das Urteil erfolgreich Berufung eingelegt (Heidtmann, „Das ist eine Privatangelegenheit des Ministers", SZ 25.02.2021, 15; siehe unten S. 144).

Brandenburg

Hartge stellt Tätigkeitsbericht 2020 vor

Die Landesbeauftragte für Datenschutz und Akteneinsicht in Brandenburg (LDABbg), Dagmar Hartge, stellte am 03.05.2021 ihren Tätigkeitsbericht 2020 vor: Von 70 Verfahren wegen Datenschutzverstößen in Brandenburg wurden Jahr 2020 16 mit der Verhängung eines Bußgelds abgeschlossen. Zahlreiche der Verfahren, die von Staatsanwaltschaften an die Datenschützerin weitergeleitet wurden, seien an andere Aufsichtsbehörden abgegeben worden. Insgesamt hat die Behörde Bußgelder in Höhe von 331.200 € verhängt: „Bußgelder orientieren sich am Einkommen von Personen und dem Umsatz von Unternehmen. Wir gehen mit Augenmaß vor. Diese Bußgelder wurden tatsächlich bezahlt und mussten nicht gesenkt werden, wozu es in

anderen Bundesländern wie im Fall von 1&1 gekommen ist." Die Umsätze seien in Brandenburg oft niedriger als in anderen Bundesländern.

Für 2020 verzeichnete die Behörde 1.322 Beschwerden, im Vergleich zum Vorjahr 2019 war das ein Anstieg um 50%. 15% mehr Datenpannen wurden gemeldet und die Zahl der Hinweise und Verwarnungen wuchs um 70%. Corona hat auch im Hinblick auf den Datenschutz dem Jahr 2020 seinen Stempel aufgedrückt, u.a. wegen des virtuellen Fernunterrichts und der vermehrten Arbeit im Homeoffice.

Aus dem Bereich der datenschutzrechtlich kontroversen Unterrichtsplattformen hob Hartge einen Fall hervor, in dem ein Schüler eine Datenpanne in der Microsoft-Cloud gemeldet hatte. Über Microsoft-Office konnte er auf persönliche Daten in vier Schulen zugreifen, darunter Schuldokumente, Unterrichtsvorbereitungen, Mails von Lehrern und deren Kontaktdaten. Lehrer hatten fälschlicherweise Benutzergruppen von privat auf öffentlich umgestellt. Die Schule hatte außerdem weder einen Vertrag zur Auftragsdatenverarbeitung geschlossen noch eine Datenschutz-Folgenabschätzung vorgenommen.

Da das Urteil des Europäischen Gerichtshofs zum Privacy Shield (DANA 3/2020, 199 ff.) auch für Schulen gilt, sprach sich Hartge kurzfristig für die Nutzung der Hasso-Plattner-Schulcloud aus, die innerhalb von fünf Tagen einsetzbar sei: „Die HPI-Schulcloud ist mit uns abgestimmt und das Feedback von Potsdamer Lehrern ist, dass sie funktioniert." Mit Microsoft verhandele ihre Dienststelle wegen der Datenschutzprobleme. Die Schulen würden sie nicht allein lösen können.

Viel diskutiert wurden im Frühjahr und Sommer 2020 auch die oft offen in Lokalen ausliegenden Gästelisten zur Kontaktnachverfolgung. Nach zahlreichen Beschwerden waren die Ergebnisse von Kontrollen in über 50 brandenburgischen Gaststätten ernüchternd: In 30 Fällen wurden mehr Daten erhoben als vorgeschrieben und in 36 Fällen haben Cafés und Restaurants die Löschfrist nicht oder zu spät umgesetzt. In Einzelfällen nutzten Betriebe die Kontaktdaten sogar vorschriftswidrig für eigene Werbezwecke.

Im Hinblick auf die Luca-App verwies die Landesdatenschützerin auf die Stellungnahme der Datenschutzkonferenz vom 29.04.2021: „Viele Themen sind vom Anbieter noch nicht so abgearbeitet, wie es nötig wäre. Die Probleme sollen binnen vier Monate abgestellt werden." Die Corona-Warn-App habe den Vorteil, dass sie schneller über ein Infektionsrisiko informieren könne, da das bei Luca über die Gesundheitsämter erfolge. Hartge plädierte für eine Ergänzung der Corona-Warn-App durch neue Funktionen.

Anfragen und Beschwerden zur Videoüberwachung stiegen 2020 erneut an auf 190. Die Landesbeauftragte berichtete, dass die Staatskanzlei während der einmonatigen EinheitsEXPO die Ausstellungsstücke in der Potsdamer Innenstadt rund um die Uhr durch Videokameras überwachen ließ. Eine Beschilderung dazu fehlte ebenso wie eine Dokumentation. Maßgaben der Datenschutzaufsichtsbehörde ignorierte die Staatskanzlei oder setzte sie nur halbherzig um, weshalb sie verwarnt wurde.

Ein weiteres Problemfeld der Videoüberwachung seien die immer beliebter werdenden Drohnen. So ließ ein Makler zur besseren Vermarktung eines Grundstückes Drohnen über die Nachbarschaft fliegen und Luftaufnahmen fertigen. Auf den Bildern, die das Unternehmen online veröffentlichte, waren auch die Nachbargrundstücke zu sehen, inklusive privater Gärten und Sonnenterrassen. Nachdem der Makler die Aufnahmen freiwillig auf seiner Website löschte, blieb es bei einem förmlichen rechtlichen Hinweis (Hottelet, Datenschutz in Brandenburg: Mehr Verfahren auch wegen Corona, www.heise.de 03.05.2021, Kurzlink: https://heise.de/-6035191)

Hessen

Videokontrolle schülerischer Sportübungen

Die Frankfurter Rundschau berichtete unter dem Titel „Hohe Hürden für Homesport" am 26.02.21 (Autor Peter Hanack, Seite D3) darüber, wie Lehrkräfte anlässlich der Corona-Pandemie und dem dadurch eingeführten Home-Schooling per Videokonferenzschaltung den Sport der Schülerinnen und Schüler kontrollieren. Dies veranlasste den DANA-Leser Wolf Göhring, uns folgenden Leserbrief zukommen zu lassen:

„Man stelle sich vor, eine Lehrerin klingelte an der Wohnungstür und begehrte aus Gründen des Unfallschutzes, schnell in der Wohnung die Sportübungen des Nachwuchses zu kontrollieren und mit ein paar Aufnahmen zu dokumentieren. Die Eltern würden der Eintrittsuchenden die Tür vor der Nase zuschlagen. Nicht weniger dreist ist die staatsschulamtliche Forderung an Lehrende, von den zumeist minderjährigen Lernenden den Videozugang zur Wohnung der Eltern abzuverlangen, um häuslich zu verrichtende Sportübungen per Video „kontinuierlich zu beobachten und ggf. zu korrigieren", wie das staatliche hessische Schulamt und die Unfallkassen schreiben. Da hat wohl Big Brother auf einigen Amtssesseln das Kommando übernommen. Wie selbstverständlich will er die garantierte Unverletzlichkeit der Wohnung so mal eben aufheben. Schon genug des Einbruchs in die Privatsphäre, dass die Lehrenden ohne auch nur im Ansatz nach einer Zustimmung der Eltern zu fragen, einzelne Unterrichtsstunden per Videokonferenz abkaspern."

Niedersachsen

Beschwerden und Bußgelder ziehen an

Gemäß Angaben der Datenschutzbeauftragten des Landes, Barbara Thiel, häufen sich in Niedersachsen die Beschwerden über Verstöße gegen den Datenschutz. Im Jahr 2020 hat ihre Behörde insgesamt 2.479 Beschwerden erhalten. Das ist fast ein Drittel mehr als im Jahr zuvor (2019: 1.882). Auch die Zahl der gemeldeten Datenschutzverstöße von Unternehmen, Vereinen und öffentlichen Stellen legte von 824 auf 989 zu.

Die Summe der 28 verhängten Bußgelder belief sich 2020 auf 10,56 Mio €. Auch das ist ein deutlicher Anstieg zum Vorjahr, als Bußgelder über insgesamt 480.000 € verhängt worden waren. Al-

lerdings ist das fast komplett auf das Bußgeld gegen notebooksbilliger.de in Höhe von 10,4 Mio. € zurückzuführen (DANA 1/2021, 45). Das Unternehmen hatte Beschäftigte und Kunden über mindestens zwei Jahre per Video überwacht, ohne dass dafür eine Rechtsgrundlage vorlag. Das Bußgeld ist noch nicht rechtskräftig.

Thiel erklärte, ihre Behörde habe ein neues Kapitel in Sachen Bußgelder aufgeschlagen und sich dabei strikt an die Datenschutz-Grundverordnung gehalten, wonach die Bußgelder „wirksam, verhältnismäßig und abschreckend" sein sollen: „Die Verarbeiter von Daten müssen verstehen, dass sie durch Fehlverhalten unter Umständen tief in das Recht auf informationelle Selbstbestimmung und damit in ein Grundrecht eingreifen. Entsprechend hoch wird, wo nötig, im Einzelfall ein von mir verhängtes Bußgeld ausfallen". Das Bußgeld gegen notebooksbilliger.de war das erste von ihr in Millionenhöhe gewesen. Endgültig vollstreckt sind von den insgesamt 10,56 Mio € jedoch erst rund 81.000 €. In den übrigen Fällen ist der Bescheid noch nicht rechtskräftig, beispielsweise, weil die Verantwortlichen Rechtsmittel dagegen eingelegt haben (Niedersachsen: Deutlich mehr Datenschutzverstöße gemeldet, www.heise.de 13.03.2021, Kurzlink: https://heise.de/-5987321).

Thüringen

Datenschutzbeauftragter gegen Bildungsminister

Der Thüringer Datenschutzbeauftrage Lutz Hasse hat ein Verfahren gegen Bildungsminister Helmut Holter eröffnet wegen eines Auftritts des Ministers via Instagram, wo er Fragen von Schülern beantwortet hatte. Hasse war kurz zuvor vom Lehrerverband hart für seine „übertriebene" Datenschutzlinie kritisiert worden.

Hasse startete am 28.01.2021 wegen einer virtuellen Instagram-Veranstaltung ein Anhörungsverfahren gegenüber dem Bildungsministerium und der Landesschülervertretung. Eine solche Anhörung kann ein erster Schritt zur Ahndung eines möglichen Datenschutzverstoßes sein, bedeutet aber noch nicht, dass es tatsächlich zu Konsequenzen kommt. Bei der Video-Schalte am 26.02.2021 ging es um Schulpolitik in Zeiten der Corona-Pandemie. Hasse erläutert: „Uns ist noch nicht klar, wer datenschutzrechtlich der Veranstalter ist." Mit der Anhörung wolle seine Behörde klären, wer wen eingeladen habe und auf wessen Initiative hin das gelaufen sei. Er wies darauf hin, dass seine Behörde das Bildungsministerium bereits im Vorfeld auf datenschutzrechtliche Bedenken bei der Veranstaltung hingewiesen habe. Instagram gehöre zu Facebook, wobei Daten zwischen den sozialen Netzwerken ausgetauscht und auch Profile erstellt würden. Im schulischen Kontext gehe das datenschutzrechtlich „gar nicht".

Seine Behörde wolle nun aber erst einmal Informationen sammeln. Es gehe dabei auch um Fragen, in welcher Funktion der Schülervertreter bei der Veranstaltung war und ob Holter als Minister oder als Privatperson teilgenommen hat: „Ich denke, dass die Verantwortlichkeit eines Schülers eine andere ist als die eines Ministers." Holter meinte „Selbstverständlich werde ich dem Datenschutzbeauftragten Auskunft geben" und betonte zugleich, dass es sich um ein Missverständnis handeln müsse: „Die Veranstaltung war weder eine schulische Veranstaltung, noch ist sie in irgendeiner Form im politischen Raum unüblich oder anstößig. Es handelte sich um politische Kommunikation."

Er verteidigte die Video-Schalte. Es sei wichtig, dass sich Schülervertretungen eigenständig engagieren und artikulieren könnten: „Es kann nicht sein, dass das demokratische Engagement von Schülerinnen und Schülern durch ein solches Vorgehen infrage gestellt oder latent mit Verfolgung bedroht wird."

Leon Schwalbe, Sprecher der Landesschülervertretung, erklärte, es gebe derzeit viele Fragen bei den Schülern: „Das weitere Home-Schooling, die Schulöffnungen für Abschlussklassen und nicht zuletzt die anstehenden Abschlussprüfungen sind Themen, bei denen eine einfache und direkte Kommunikation nötig ist, um Klarheit zu schaffen." Mit dem Instagram-Livestream mit Holter habe man diese Möglichkeit geben wollen. „Die sozialen Medien sind für die Landesschülervertretung aufgrund der jungen Zielgruppe seit vielen Jahren ein wichtiges Kommunikationsmittel. Eine Einschränkung dieser Aktivität würde unsere ganze Arbeit behindern."

Kritik am Vorgehen des Landesdatenschutzbeauftragten kam von der Landeselternvertretung. Sie warf Hasse „unsensibles Agieren" vor. Die Eltern hätten sich gewünscht, dass der Datenschutzbeauftragte dasselbe Engagement gezeigt hätte, als es um klare Regeln und eine Liste sicher nutzbarer Kommunikationswege für Schüler, Eltern und Schule ging. Die CDU im Landtag forderte ein Machtwort von Holter. Der bildungspolitische Sprecher der Fraktion, Christian Tischner, sagte, Holter müsse sich „endlich klar und unmissverständlich vor Lehrer und Schüler stellen". Windelweiche Lippenbekenntnisse genügten nicht.

Der Datenschutzbeauftragte Hasse war für seine digitale Strategie in die Schusslinie geraten. Insbesondere Pädagogen warfen ihm vor, seine Datenschutzanforderungen zu übertreiben. Der Lehrerverband hatte Mitte Januar 2021 kritisiert, dass Schulen einzig die Schulcloud nutzen dürfen, Bildungsminister Helmut Holter sich aber zum Live-Gespräch auf der zum amerikanischen Facebook-Konzern gehörenden Plattform Instagram ankündigt. Das lasse jeden Vorbildcharakter vermissen, so Rolf Busch vom Verband damals. Hasse hatte Mitte 2020 Bußgelder für den Fall angedroht, dass Lehrer auf Kommunikationsplattformen zurückgreifen, die von der datenschutzrechtlich gesicherten Schulcloud abweichen (DANA 3/2020, 193). Die Cloud bereitet Thüringer Lehrkräften und Schülern regelmäßig Probleme. In anderen Bundesländern wird aus ähnlichen Gründen auf andere, unter anderem private Plattformen zurückgegriffen, wogegen sich Lutz Hasse für Thüringen aber ausgesprochen hat (Datenschutz: Verfahren gegen Bildungsminister Holter eröffnet, www.mdr.de 29.01.2020).

Datenschutznachrichten aus dem Ausland

Weltweit

WHO plant globales Impfzertifikat

Die Weltgesundheitsorganisation (WHO) und Estland arbeiten an einem Impfzertifikat, das von „Eritrea bis Singapur“ gültig sein soll. Gemäß der estnischen Entwicklerfirma soll das Zertifikat auf dem Smartphone gespeichert und auf Reisen von Grenzbeamten ausgelesen werden können. Dafür müssen Gesundheitsdatenbanken, Impfstoffhersteller und Impfstellen miteinander vernetzt werden. Datenschützer kritisieren, dass sich dadurch Geimpfte sowie deren Kontakte und Gesundheitsstatus überwachen ließen. Estland will das verhindern, indem es die Daten dezentral mit Hilfe von Blockchain-Technologie speichert und damit das System vor Hackerangriffen und Manipulation schützt.

Estand gilt seit Langem als Vorreiter der Digitalisierung. Für den Impfpass werden Erfahrungen mit dem estnischen System „X-Road“ genutzt. Es besteht aus dezentralen Datenbanken, Programmen und Rechtsvorschriften und wird z.B. bei virtuellen Behördengängen oder Wahlen genutzt. Nur wenige Länder experimentieren bislang mit elektronischen Impfpässen. Ob Geimpfte Privilegien bekommen sollen, ist umstritten. In Deutschland wird dies bisher abgelehnt; andere Länder diskutieren die Frage ausführlicher. Griechenland und Israel schlossen ein Abkommen, das immunisierten Staatsbürgern Reisen zwischen den beiden Ländern ohne Quarantänepflicht erlauben soll. Auch dafür ist ein digitaler Impfpass geplant (Globaler Impfpass, Der Spiegel Nr. 7 13.02.2021, 71).

Weltweit

Spanier und Österreicher am datenschutzsensibelsten

Rund 41% der Deutschen versuchen ihre Daten im Internet aktiv zu schützen. Das geht aus einer Befragung im Rahmen des Statista Consumer Survey 2020 hervor. Demnach sind die Deutschen vergleichsweise vorsichtig was den Umgang mit sensiblen Daten angeht. Den Spitzenwert im europäischen Vergleich erzielen die spanischen Befragten – hier bemühen sich rund 45 Prozent persönliche Informationen zu schützen. Weniger Wert auf aktiven Datenschutz legen die Befragten aus Frankreich (31,3 Prozent) und Südkorea (20,9 Prozent). Alle Zahlen in Prozent:

Spanien	45,0
Österreich	42,2
Deutschland	41,4
China	40,9
Schweiz	40.4
USA	35,3
Großbritannien	32,7
Russland	32,4
Frankreich	33,3
Südkorea	20.9

(Bocksch, Vier von zehn Deutschen schützen ihre Daten, 08.02.2021)

Weltweit

„Harmlose“ geklaute Bilder auf Pädosexuellen-Foren

Harmlose Alltagsfotos von Kindern, die von Eltern und Kindern in den Sozialen Medien veröffentlicht werden, stehen verstärkt im Fokus von Pädosexuellen. Gemäß einer umfangreichen journalistischen Recherche beschaffen sich die Täter massenhaft Aufnahmen aus privaten Social-Media-Profilen, um sie anschließend in Foren hochzuladen, in denen auch Fotos getauscht werden, die schweren Kindesmissbrauch zeigen. Allein auf einer der größten illegalen Foto-Plattformen für Pädosexuelle stammt mindestens jedes vierte Bild ursprünglich von Facebook oder Instagram. Häufig werden die Aufnahmen obszön kommentiert, manchmal nennen die Täter auch Namen und Alter des Kindes und verlinken sogar die ursprünglichen Social-Media-Profile.

Ermittlungsbehörden und Kinderschutz-Organisationen appellieren seit Jahren, keine Kinderfotos im Internet zu teilen. Das Interesse von Pädosexuellen an solchen harmlosen Bildern von Mädchen und Jungen etwa beim Sport oder am Strand ist groß. Ein Recherche-Team von Panorama und STRG_F klärte die Herkunft von vielen Aufnahmen auf einschlägigen Plattformen. Dafür hat es automatisiert mehrere Millionen Fotos untersucht. In Hunderttausenden Fällen konnte es nachweisen, dass die Fotos ursprünglich von Facebook- und Instagram-Accounts stammen. Beide Dienste speichern in Metadaten einen eindeutigen Hinweis in jeder Bilddatei, der erhalten bleibt, wenn das Bild an anderer Stelle unverändert hochgeladen wird. In vielen Foren fanden sich auch Anhaltspunkte auf YouTube, TikTok und WhatsApp als Quelle der gestohlenen Bilder.

„Pädophilie“ bezeichnet die sexuelle Präferenz, aus der sich Handlungsimpulse ergeben können, aber nicht müssen. Kommt es zu sexuellen Handlungen, also zu real ausgelebter Sexualität mit Kindern, spricht man von „Pädosexualität“, womit Kindesmissbrauch einhergeht. Täter, die auf Plattformen Kinderbilder konsumieren und sexualisiert kommentieren, sind in diese Kategorie einzuordnen.

So treffen sich auf der Plattform „Cutie Garden“ (deutsch etwa „Garten der Süßen“) Pädosexuelle und posten und kommentieren auf diesem sogenannten Imageboard anonym Fotos von Kindern. Das Rechercheteam analysierte 142.381 Fotos und fand bei rund 23,5% den eindeutigen Hinweis, dass das Foto von Facebook oder Instagram stammt. Die Dunkelziffer dürfte höher liegen, weil manche User die Hinweise in den Metadaten gezielt verwischen.

Recherchen im Bereich von Kinderpornografie sind heikel, da nicht nur der Besitz solcher Aufnahmen strafbar ist, sondern schon das bloße Ansehen dieser Fotos und Videos. Wer sich in dieser Umgebung aufhält, kann sich schnell strafbar machen. Wegen des Interesses der Öffentlichkeit, über solche Gefahren für das Kindeswohl unabhängig und anschaulich informiert zu werden, können journalistische Recher-

chen zulässig sein, vorausgesetzt sie dienen ausschließlich diesen journalistischen Zwecken. Panorama mietete für mehrere Monate einen streng abgeschirmten Raum in der Bundespressekonferenz in Berlin an, zu dem nur ausgewählte Personen Zutritt hatten. Alle Computer und Server waren mehrfach verschlüsselt, um auszuschließen, dass unbefugte Personen in Besitz des Materials kommen. Ziel war es, die scheinbar harmlosen Alltagsfotos von Kindern herunterzuladen, um anschließend ihre Herkunft zu erklären. Illegales Material, insbesondere Missbrauchsfotos und -videos, wurden nicht heruntergeladen.

Dabei entdeckte das Recherche-Team zahlreiche Alltagsbilder von Kindern in einschlägigen Kinderpornografie-Foren im so genannten Darknet. Dort werden sie in besondere Kategorien wie „Non Nude" („nicht nackt") hochgeladen. Die Reporterinnen und Reporter konnten gleich mehrere Fälle deutscher Kinder identifizieren, deren Aufnahmen ursprünglich von Instagram oder YouTube stammten. Darunter ein Video, das zwei Jungen beim harmlosen Versteckspiel zeigt. In den Kommentaren fantasierten User über Analverkehr mit den Kindern, einer schrieb: „Und dann mache ich sie zu meinen Sex-Sklaven." Die jeweils betroffenen Eltern, konfrontiert mit den Rechercheergebnissen, zeigten sich erschüttert und löschten teilweise ihre Social-Media-Profile.

Eltern und Jugendliche helfen Pädosexuellen mit ihren geposteten harmlosen Aufnahmen oft unfreiwillig dabei, an neue Missbrauchsfotos zu kommen: Wer als User neue Bilder in den Kinderpornografie-Foren postet, zum Beispiel, nachdem er sie in sozialen Netzwerken geklaut hat, erhält mehr Anerkennung und mehr Bilder von anderen Usern. User zahlen in den Foren nicht mit Geld, sondern mit Fotos und Videos, die sie anderen wiederum zur Verfügung stellen.

Ein besonderer Fall ist die russische Foto-Plattform „imgsrc.ru", die über das gewöhnliche Internet erreichbar ist und von Pädosexuellen für ihre Zwecke genutzt wird. Dort identifizierte das Reporterteam in der Kategorie „Kids" über drei Millionen Aufnahmen, die meisten davon offensichtlich geklaut. Den Ergebnissen der Analyse nach wurden sie schon über 14 Milliarden mal geklickt, häufiger als die Bilder aller anderen Kategorien – etwa Natur-, Auto- und Städtefotos – zusammen. Auffallend viele User kommentieren die Fotos auf Deutsch. Ein Nutzer schrieb z.B. unter ein Bild, das von der Seite eines sächsischen Sportvereins gezogen wurde und ein junges Mädchen bei einer Turnübung zeigt: „Diesen Blick hat sie auch, wenn ich ihn ihr bis zum Anschlag reinschieben würde."

Andreas Link von jugendschutz.net, dem gemeinsamen Kompetenzzentrum von Bund und Ländern für Jugendschutz im Internet, weist darauf hin, dass Eltern und Jugendliche, die Fotos im Internet posten, es Tätern oft sehr einfach machen, diese für ihre Zwecke zu nutzen: „Pädosexuelle sind Jäger und Sammler, die gezielt solche Alltagsbilder suchen. Und wenn Eltern und Jugendliche diese Fotos im Internet posten, dann machen sie es den Tätern oft sehr einfach, diese für ihre Zwecke zu nutzen. Einmal im Netz sind sie dort für immer verfügbar." Das Rechercheteam entdeckte auch Fälle, in denen Bilder von nicht-öffentlichen Social-Media-Profilen kopiert wurden. Dies könnte dadurch zu erklären sein, dass die Opfer unter ihren Freunden und Followern Personen haben, die die Fotos ohne ihr Wissen kopierten und veröffentlichten.

Facebook und Instagram verwiesen auf Nachfrage auf die angebotenen Privatsphäre-Einstellungen: „Wir unterstützen Eltern dabei zu entscheiden, mit wem sie ihre Alltagsbilder teilen möchten." Das Herunterladen von Userdaten verstoße generell gegen die Richtlinien. Man verfüge darüber hinaus über Technologie, die proaktiv Nacktheit und ausbeuterische Inhalte von Kindern beim Hochladen erkenne. YouTube teilte mit, dass man stark in Technologie investiere, die Kindern und Familien den bestmöglichen Schutz biete.

Staatsanwältin Julia Bussweiler von der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) erklärte zum Diebstahl von Alltagsfotos von Kindern aus sozialen Medien: „Es ist erschreckend, wie häufig solche Alltagsbilder missbraucht und gegen den Willen der Abgebildeten verwendet werden." Die Behörden würden nur in den seltensten Fällen aktiv, wenn sie Alltagsbilder in Kinderpornografie-Foren entdecken, da die Aufnahmen an sich nicht strafbar sind, strafrechtlich relevant seien dagegen die Kommentare, die etwa eine sexuelle Handlung beschreiben. Wohl könnte jeder Abgebildete das Recht am eigenen Bild geltend machen: „Dafür bräuchte es eine Anzeige der Eltern, aber die wissen zumeist gar nicht, dass ihre Fotos geklaut und in entsprechende Plattformen hochgeladen wurden. Das ist ein Problem." Der sicherste Schutz für Kinder und Jugendliche sei es deshalb, gar keine Bilder offen ins Netz zu stellen (Bongen/Güldenring/Lenz/Moßbrucker, Geklaut: Private Kinderfotos auf Kinderpornografie-Seiten, www.ndr.de 22.04.2021).

Weltweit

Große Sicherheitsmängel bei Amazon

Amazon ist einer der großen Akteure im Big-Data-Bereich. Drei frühere führende Mitarbeiter aus dem Bereich IT-Sicherheit berichten, dass dem US-Konzern als Gegengewicht jeglicher Ansatz für eine effektive Datenschutzkultur fehlt. Es existierten nicht einmal die grundlegenden Voraussetzungen, um die Privatsphäre der Nutzer angemessen zu schützen. Dies dürfte früher oder später zu massiven Folgen wie einem unkontrollierbaren Datenabfluss führen und könnte Hackern Angriffe erleichtern.

Die Warnungen stammen von zwei Ex-Beschäftigten in den USA sowie einem aus Europa. Alle drei sollen demnach wiederholt versucht haben intern die Führungsebene in der Zentrale in Seattle zu alarmieren. Sie seien aber beiseite geschoben, entlassen oder aus dem Unternehmen gedrängt worden. Das Hauptproblem besteht ihnen zufolge darin, dass der Online-Händler Zehntausende Teams auf Big-Data-Analysen ansetze. Den Mitarbeitern und der Konzernspitze sei aber überhaupt nicht klar, welche Daten vorlägen, wo sie gespeichert sind und wer Zugriff darauf hat.

Den in der Datenschutz-Grundverordnung (DSGVO) oder auch im kalifornischen Pendant verankerten Nutzerrechten etwa auf Auskunft und Korrektur könne das Unternehmen den Whistleblowern zufolge so gar nicht nach-

kommen. Wenn etwa ein Kunde seinen Löschanspruch nach dem „Recht auf Vergessenwerden" ausüben wolle, wäre es für Amazon nahezu unmöglich, alle Stellen ausfindig zu machen, an denen sich die persönlichen Daten in verschiedenen Systemen befänden.

Einer der Insider: „Wir haben Hunderttausende von Konten gefunden, bei denen der Mitarbeiter nicht mehr da ist, aber immer noch Zugriff auf das System hat." Laut internen Sicherheitsberichten aus 2016 und 2017 habe das Unternehmen angegeben, nur zwischen 55% und 70% seiner Systeme mit Sicherheitsupdates versorgen zu können. In einem internen Memo von 2018 sei die Wahrscheinlichkeit eines kritischen finanziellen Verlusts oder eines Imageschadens für das Unternehmen als „sehr hoch" eingeschätzt worden, da es nicht möglich sei Angriffe von Gegnern zu identifizieren.

Die Rede ist auch vom Einsatz eines unsicheren Verschlüsselungsprotokolls für Online-Zahlungen seit 2014. Das Problem sei erst nach weiteren Hinweisen 2016 und 2018 behoben worden. Zuvor habe Amazon erfolgreich Lobbyarbeit beim zuständigen Standardisierungsgremium betrieben und zwei Jahre Aufschub gewährt bekommen. Der Konzern, der bisher vor allem wegen mangelndem Arbeitnehmerschutz in der Kritik steht, soll zudem erst wenige Wochen vor der Anwendbarkeit der DSGVO im Frühjahr 2018 ein spezielles Team für die Umsetzung der Vorgaben eingerichtet haben. Deutlich mehr Wert lege Amazon auf die IT-Sicherheit bei seinem Cloud-Flaggschiff AWS. Dortige Datenlecks seien in der Regel auf nachlässige Nutzer zurückzuführen.

In der EU ist hauptsächlich die luxemburgische Datenschutzaufsichtsbehörde für den Konzern zuständig. Die bestätigte nur allgemein, dass Verfahren gegen Amazon anhängig sind. Erste Bußgelder hätten eigentlich 2020 fällig werden sollen, es sei aber zu Verzögerungen gekommen. Ein Unternehmenssprecher wies die Vorwürfe zurück. Bei Amazon gehöre es seit Jahren zu den obersten Prioritäten die Privatsphäre der Kunden zu schützen und die Sicherheit ihrer Daten zu gewährleisten. Dafür gebe es lang etablierte Richtlinien und Verfahren. Die Behauptungen seien „ungenau, unbegründet und veraltet" (Krempl, Amazon: Whistleblower sehen Millionen von Kundendaten in Gefahr www.heise.de 25.02.2021, Kurzlink: https://heise.de/-5065861).

Europa

EU-Kommission plant KI-Regulierung

Die EU-Kommission stellte am 21.04.2021 eine Strategie vor, wie die Entwicklung von sog. Künstlicher Intelligenz (KI) als wissenschaftlicher und wirtschaftlicher Hoffnungsträger gefördert werden kann und zugleich die damit einher gehenden Risiken begrenzt werden können. Selbstlernende Computerprogramme, die ihre Leistung durch die Analyse großer Datenmengen stetig verbessern, sind ein wirkmächtiges Werkzeug und eine Zukunftstechnologie, bei der Europa von den USA und China abgehängt zu werden droht.

Die für Digitales zuständige Kommissarin und Vizepräsidentin Margrethe Vestager präsentierte einen 81-seitigen Verordnungsvorschlag, der gewisse Anwendungen künstlicher Intelligenz verbietet und andere strengen Regeln unterwirft: „Bei künstlicher Intelligenz ist Vertrauen ein Muss und kein Beiwerk." Eine Verordnung gilt unmittelbar in allen Mitgliedstaaten. Vorgesehen ist eine kurze Liste von Anwendungen, die grundsätzlich verboten sind, es sei denn, Regierungen nutzen sie unter gewissen Umständen zum Schutz der Bevölkerung. Auf der Liste steht die wahllose Überwachung von Bürgern oder der Versuch, die Meinung oder das Verhalten von Menschen mit Hilfe ausgeklügelter Algorithmen zu manipulieren.

So will die Kommission nach entsprechender Kritik von Abgeordneten im Europaparlament die Verwendung von KI bei automatischer Gesichtserkennung auf öffentlichen Plätzen einschränken. Demnach wird der Polizei verboten KI-Systeme in Echtzeit die Bilder von Überwachungskameras durchsuchen zu lassen. Zeitlich und geografisch begrenzte Ausnahmen sollen möglich sein, wenn ein Richter sie genehmigt und diese z.B. dazu dienen einen Terroranschlag zu verhindern oder bei der Suche nach einem vermissten Kind oder einem gefährlichen Verbrecher zu helfen.

Daneben gibt es eine deutlich längere Aufstellung sogenannter „Hoch-Risiko"-Systeme. Diese Anwendungen sollen unter strengen Auflagen erlaubt werden. So müssen die Daten für das Trainieren der Software von hoher Qualität sein, die Arbeitsweise der KI muss transparent sein, und die Programme müssen von Menschen überwacht werden. Firmen und Staaten dürfen KI-Software nicht einsetzen, um Menschen „mit sublimen Techniken, ohne dass sich die Person dessen bewusst ist", zu manipulieren oder um Social Scoring zu betreiben. Hier geht es z.B. um KI-Programme, welche die Kreditwürdigkeit von Menschen benoten, Stellenbeschreibungen vorsortieren oder beim Betrieb des Strom- oder Gasnetzes eingesetzt werden. Bei solchen riskanten Anwendungen verlangt das Gesetz, dass die Daten, die zum Trainieren der Systeme verwendet werden, hochwertig sind und nicht bestimmte Gruppen diskriminieren. Menschen müssen die Software einfach überwachen und zur Not ausschalten können; die Arbeitsweise der Programme muss transparent sein. Bei schweren Verstößen soll eine Strafe von bis zu 6% des weltweiten Umsatzes möglich sein. Vestager meinte: „Mit diesen wegweisenden Vorschriften steht die EU an vorderster Front bei der Entwicklung neuer weltweiter Normen." Mit dem Gesetz „können wir weltweit den Weg für ethische Technik ebnen".

Alexandra Geese, die das Thema für die Grünen betreut, klagte, der Entwurf sei „an entscheidenden Stellen nicht scharf genug". Auf der anderen Seite moniert der CSU-Europaabgeordnete Markus Ferber, der wirtschaftspolitische Sprecher der christdemokratischen EVP-Fraktion, dass sich der Vorschlag „wie ein Verbotskatalog" lese: „Im Bereich der Künstlichen Intelligenz gibt es viele Anwendungsfälle, die sich heute noch gar nicht absehen lassen. Wenn die Kommission zu restriktiv reguliert, droht sie einer Zukunftstechnologie den Hahn abzudrehen, bevor wir ihr Potenzial jemals richtig ausschöpfen konnten" (Finke, Hoffnung und Furcht, SZ 15.04.2021, 19; Finke, Mächtige Technik, strenge Regeln, SZ 22.04.2021, 15).

Europa

Parlamentarier: Datenschutzaufsicht besser ausstatten

Der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des EU-Parlaments fordert eine wirksamere Durchsetzung der Datenschutz-Grundverordnung (DSGVO) und kritisiert, dass viele Aufsichtsbehörden in der EU nicht über ausreichende personelle, technische und finanzielle Ressourcen verfügen, um ihre Aufgaben zu erfüllen und ihre Befugnisse effektiv auszuüben. Die Kontrollinstanzen sollten in der Lage sein eine wachsende Zahl ressourcenintensiver und komplexer Fälle schnell und gründlich zu bearbeiten.

In einem am 16.03.2021 mit 41 zu 2 Stimmen bei 24 Enthaltungen angenommenen Entschließungsentwurf appelliert das Gremium vor allem an die irischen und luxemburgischen Datenschutzbehörden ihre laufenden Ermittlungen in wichtigen Fällen zu beschleunigen. Vor allem die irische Data Protection Commission (DPC) gilt als chronisch unterbesetzt sowie voreingenommen und kommt in den von ihr eingeleiteten großen internationalen Verfahren nur langsam voran. Sie ist für Internetkonzerne wie Facebook, Google und Twitter zuständig, da diese ihren europäischen Hauptsitz in Irland haben.

Bei den Luxemburger Prüfern sind unter anderem Verfahren gegen Amazon anhängig. Erste Bußgelder hätten eigentlich 2020 verhängt werden sollen, es kam aber auch hier zu Verzögerungen. In Deutschland klagt vor allem der Datenschutzbeauftragte von Mecklenburg-Vorpommern, Heinz Müller, über eine unangemessene Personalausstattung. Er war daher Ende 2019 aus der SPD ausgetreten. Der Kontrolleur hatte nach eigenen Angaben zu den 21 vorhandenen Stellen 13 weitere beantragt, um die mit der DSGVO verknüpften neuen Aufgaben zu bewältigen, aber keine bewilligt bekommen.

Der Innenausschuss macht sich ferner dafür stark die Zusammenarbeit zwischen den nationalen Aufsichtsbehörden im Europäischen Datenschutzausschuss (EDSA) stärker zu koordinieren und zu erleichtern. Es falle auf die einzelnen Bürger zurück, wenn die Kooperation im EDSA nicht angemessen funktioniere. Darüber hinaus habe die Covid-19-Pandemie deutlich gemacht, dass die nationalen Datenschutzbehörden und der EDSA klare Anweisungen geben müssten, wie die DSGVO in der öffentlichen Gesundheitspolitik angemessen umzusetzen sei. Da die Anwendung des Normenwerks für kleine und mittlere Unternehmen (KMU) und einige andere Organisationen wie Schulen und Vereine eine besondere Herausforderung darstelle, fordern die Parlamentarier „mehr Unterstützung, Informationen und Schulungen“.

Insgesamt halten die Innenpolitiker die DSGVO aber für einen Erfolg. Der Ausschuss hält es aktuell nicht für notwendig, die Verordnung zu aktualisieren oder generell zu überprüfen. Unter anderem der CDU-Abgeordnete Axel Voss hatte zuvor auf eine zeitnahe Reform gedrängt (Krempl, DSGVO: EU-Abgeordnete mahnen bessere Datenschutz-Durchsetzung an, www.heise.de 16.03.2021, Kurzlink: https://heise.de/-5989653).

Europa

EU-Parlament bewertet DSGVO-Umsetzung kritisch

Das EU-Parlament hat die Umsetzung der Datenschutz-Grundverordnung (DSGVO) in den EU-Mitgliedstaaten in einer am 25.03.2021 beschlossenen Entschließung beanstandet. Man sei besorgt über die uneinheitliche und teils nicht vorhandene Durchsetzung knapp drei Jahre nach Anwendbarkeit. So sei nur ein sehr kleiner Teil eingereichter Beschwerden weiterverfolgt worden. Außerdem seien verhängte Geldstrafen gegen große Unternehmen teils zu gering, um Wirkung zu zeigen.

Das Parlament kritisierte, dass es noch keine Vertragsverletzungsverfahren gegen Mitgliedstaaten gebe, die ihren Verpflichtungen aus der DSGVO nicht ausreichend nachkämen. EU-Justizkommissar Didier Reynders versicherte in der Plenardebatte, die Kommission scheue davor nicht zurück. Er betonte zudem, dass kleine und mittlere Unternehmen bei der Umsetzung der Regelungen besser unterstützt werden sollten.

Die Abgeordneten monierten, dass die Verordnung teils zur Einschränkung der Presse und nichtstaatlicher Organisationen missbraucht werde. Für eine grenzüberschreitende Kooperation fehlten den zuständigen Aufsichtsbehörden in einigen Mitgliedstaaten zudem die notwendigen Ressourcen. Insgesamt wertete das Parlament die DSGVO aber als Erfolg.

Die Abgeordneten sprachen sich für eine Art Schengenraum für Daten in der EU aus, der auf europäischen Werten wie Transparenz, Datenschutz und der Achtung der Grundrechte basiere. Daten sollten etwa durch Standardisierungen besser teilbar und nutzbar werden. Ein freier Datenfluss in der EU solle auch die Wettbewerbsfähigkeit etwa von europäischen Unternehmen stärken (Europaparlament kritisiert Umsetzung der DSGVO, www.horizont.at 26.03.2021).

Europa

Datenschützer kritisieren Entwurf eines Data Governance Act

Der Europäische Datenschutzausschuss (EDSA) und der EU-Datenschutzbeauftragte Wojciech Wiewiórowski fordern in einer gemeinsamen Stellungnahme umfangreiche Korrekturen am Entwurf der EU-Kommission für einen Data Governance Act (DGA). Sie vermissen in der Initiative grundlegende Regelungen zur Sicherung der Privatsphäre der Bürger. Der Gesetzgeber müsse unmissverständlich klarstellen, dass der Rechtsakt „weder das Schutzniveau der personenbezogenen Daten natürlicher Personen beeinträchtigen noch die in den Datenschutzvorschriften festgelegten Rechte und Pflichten ändern wird“.

Die EU-Kommission will die öffentliche Verwaltung, Firmen und Individuen mit ihrem Vorschlag ermuntern ihre Daten stärker zu teilen. Für Bereiche wie vernetzte Autos oder das Internet der Dinge plant die Kommission entsprechende Pflichten. Das Sammeln von Messwerten zum Allgemeinwohl soll über einen gemeinsamen Ansatz für Datenspenden in allen Mitgliedstaaten befördert werden. Treuhänder sind als vertrauenswürdige Vermittler vorgesehen.

Wiewiórowski und EDSA meinen, der Begriff Datenaltruismus und die davon begünstigten Zwecke müssten besser definiert werden. Das bislang schwammige Konzept sollte so angelegt werden, „dass Einzelpersonen ihre Zustimmung leicht erteilen, aber auch zurückziehen können". Angesichts der absehbaren Risiken für Personen, deren Informationen von Austauschdiensten und von Organisationen für Datenaltruismus verarbeitet werden, gehen der EDSA und Wiewiórowski davon aus, dass eine reine Registrierung dieser Einrichtungen im Einklang mit der Datenschutz-Grundverordnung (DSGVO) nicht ausreicht. Hier müsse ein strengeres Prüfverfahren greifen. Dabei sollten Rechenschaftsinstrumente wie ein Verhaltenskodex oder ein Zertifizierungsverfahren systematisch einbezogen werden.

Bei dem noch kaum erprobten Werkzeug der Treuhänder betonen die Kontrolleure, dass die Betroffenen vorab über deren Sinn und Zweck aufzuklären seien. Zudem müssten die Vermittler die Grundsätze des Datenschutzes durch Technik („Privacy by Design") und datenschutzfreundliche Voreinstellungen, der Transparenz und der Zweckbindung berücksichtigen. Ferner sollten die Modalitäten geklärt werden, nach denen solche Diensteanbieter Einzelpersonen bei der Ausübung ihrer Rechte wirksam unterstützen könnten.

Bei der geplanten Weiterverwendung personenbezogener Daten, die öffentliche Stellen etwa im Gesundheitssektor erhoben haben, müssten die Vorschriften aus der DSGVO und der Open-Data-Richtlinie beachtet und aneinander angeglichen werden. Ein solcher Ansatz sei auch nur dann zulässig, wenn er eine Basis im EU-Recht oder in Gesetzen der Mitgliedsstaaten habe. Enthalten sein sollte eine Liste klarer, kompatibler Zwecke, für die persönliche Daten weiterverarbeitet werden dürften im Sinne beispielsweise einer „notwendigen und verhältnismäßigen Maßnahme in einer demokratischen Gesellschaft".

Allgemein erkennen die Verfasser das legitime Ziel des DGA an „die Bedingungen für den Datenaustausch im Binnenmarkt zu verbessern". Gleichzeitig sei der Schutz personenbezogener Daten aber „ein wesentlicher und integraler Bestandteil für das Vertrauen in die digitale Wirtschaft". Wiewiórowski unterstrich, dass mit Big Data eine „große Verantwortung" einhergehe. Die EDSA-Vorsitzende Andrea Jelinek hob hervor: „Die DSGVO ist das Fundament, auf dem das europäische Data-Governance-Modell aufgebaut werden muss" (Krempl, EU-Datenschützer: Bauchschmerzen beim geplanten Datenaltruismus, www.heise.de 12.03.2021, Kurzlink: https://heise.de/-5078665).

Europa

EU-Kommission meint: britischer Datenschutz ist adäquat

Persönliche Daten sollen gemäß den Vorstellungen der Kommission der Europäischen Union (EU) nach dem britischen Ausscheiden aus der EU weiter problemlos zwischen der EU und Großbritannien fließen können. Deshalb leitete die Brüsseler Behörde am 19.02.2021 ein Verfahren ein, um den Briten einen gleichwertigen Datenschutz zu bescheinigen. Bis Ende Juni 2021 gilt noch eine Übergangsphase.

EU-Kommissionsvize Vera Jourova meinte, Großbritannien habe zwar die EU verlassen, aber nicht die europäische Datenschutzfamilie: „Die Sicherstellung eines freien und sicheren Verkehrs personenbezogener Daten ist von wesentlicher Bedeutung für die Unternehmen und die Bürgerinnen und Bürger auf beiden Seiten des Ärmelkanals." Damit die Daten weiter ungehindert fließen können, müssen die EU-Staaten der Empfehlung der EU-Kommission noch zustimmen. Zuvor wird eine Stellungnahme des Europäischen Datenschutzausschusses eingeholt. Nach vier Jahren soll das Datenschutzniveau in Großbritannien erneut überprüft werden.

Ähnliche Beschlüsse hat die EU auch mit Blick auf andere Länder wie Argentinien, Japan, die Schweiz oder Neuseeland getroffen. Diesmal ist die Lage jedoch anders, weil in Großbritannien bis vor kurzem noch die EU-Datenschutzregeln galten, das Land nun aber nicht mehr darunter fällt. Aus Sicht der EU-Kommission besteht die Gefahr, dass London in den kommenden Jahren vom gemeinsamen Standard abweicht. Deshalb gebe es strenge Überwachungs- und Überprüfungsverfahren sowie die Möglichkeit zur Aussetzung oder Aufhebung derartiger Beschlüsse. EU-Justizkommissar Didier Reynders verwies darauf, dass der Datenfluss auch für eine wirksame Zusammenarbeit im Kampf gegen Kriminalität wichtig sei (EU-Kommission bescheinigt Großbritannien gleichwertigen Datenschutz, www.finanzen.net 19.02.2021).

Europa

Verbraucherverbände gegen TikTok

Der Europäische Verbraucherverband BEUC (Bureau Européen des Unions des Consommateurs), die Dachorganisation von 44 europäischen Verbraucherschutzorganisationen, hat bei der EU-Kommission Beschwerde gegen TikTok eingereicht. Die bei Minderjährigen beliebte Plattform zum Teilen von Videos verstoße gegen europäisches Recht, indem sie Kinder Schleichwerbung sowie unangemessenen Inhalten aussetze. Verbände aus 15 Ländern hatten ihren Dachverband aufgerufen, gegen das Social-Media-Unternehmen vorzugehen.

Die erhobenen Vorwürfe sind Irreführung, Täuschung, Verstöße gegen Urheber- und Datenschutzrecht sowie gegen eine Reihe von EU-weit gültigen Kinderschutzgesetzen. Mit dem Vorstoß möchten die Verbraucherschützer nach eigenen Angaben eine umfassende Ermittlung durch die zuständigen Justizbehörden in Gang setzen und geltendes EU-Recht gegenüber TikTok durchsetzen. Ein europaweites Verbot der Plattform ist damit nicht angestrebt, es geht aber um die Kerninhalte der Plattform.

Monique Goyens, Director General des Verbraucherdachverbands BEUC, stellte fest, dass TikTok bei Kindern ausgesprochen beliebt sei, und kritisierte, dass das Unternehmen den Kinderschutz außen vor lasse: „Wir wollen nicht, dass unsere Jüngsten eindringlicher Schleichwerbung ausgesetzt sind und ohne ihr Wissen zu Werbeflächen werden, während sie doch nur Spaß haben wollen." TikTok bringt nicht nur Spaß. So war im Januar 2021 ein zehnjähriges Mädchen vermutlich bei einer TikTok-

Mutprobe ums Leben gekommen: Offenbar hatte sie versucht, bei einer sogenannten „Blackout Challenge" für ein Kurzvideo mitzumachen und sich dabei mit einem Gürtel erstickt. Seither haben Datenschutzbehörden sich mit zunehmender Vehemenz für Alterseinschränkungen bei TikTok ausgesprochen.

Verstöße sehen Monique Goyens und die von ihr vertretenen Verbände vor allem in vier Punkten: TikTok habe unfaire Geschäftsbedingungen (Terms of Service), die Nutzer benachteiligten und ihnen das Recht an ihren veröffentlichten Inhalten ohne Gegenleistung „unwiderruflich" entzögen, wie es in der im Internet veröffentlichten Stellungnahme heißt. TikTok bietet laut BEUC auch gezielt Marketingangebote an, in denen Kinder und Jugendliche versteckter Werbung ausgesetzt sind – oft setzen bekannte Influencer „gebrandete Challenges" in Gang und verschleiern dabei die kommerziellen Absichten. Auch seien Kinder bei TikTok nicht geschützt vor anzüglichen, nicht jugendfreien Videos.

Den überwiegend minderjährigen Nutzern bietet TikTok virtuelle Münzen zum Kauf an, mit denen sie durch den Einsatz von echtem Geld virtuelle Geschenke für von ihnen verehrte Prominente erwerben können. In der „Virtual Item Policy" seien unfaire Bedingungen und irreführende Klauseln enthalten. So könne das Unternehmen jederzeit den Wechselkurs für Transaktionen zu eigenen Gunsten manipulieren. Die Plattform sammele persönliche Daten auf intransparente Weise; die Hinweise zur Verarbeitung seien irreführend. In diesem Punkt ermitteln offenbar bereits einige nationale Datenschutzbehörden gegen die Betreiber der Videoplattform (vgl. DANA 1/2020, 57 f.).

Der an der Aktion beteiligte deutsche Verbraucherverband Verbraucherzentrale Bundesverband (vzbv) hat nicht die deutschen Behörden eingeschaltet, sondern stattdessen TikTok juristisch verwarnt. An der formalen Beschwerde bei der EU-Kommission beteiligen sich folgende Verbände: Test Achats/Test Ankoop (Belgien), Kypriakos Syndesmos Katanaloton/CCA (Zypern), dTEST (Tschechien), Forbrugerrådet Tænk (Dänemark), UFC Que Choisir (Frankreich), vzbv (Deutschland), EKPIZO (Griechenland), Altroconsumo, Consumatori Italiani per l'Europa/CIE (Italien), Consumentenbond (Niederlande), Forbrukerradet (Norwegen), Spoločnosť ochrany spotrebiteľov (S.O.S.) Poprad (Slowakei), Zveza Potrošnikov Slovenije/ZPS (Slowenien), Sveriges Konsumenter (Schweden), ASUFIN, Organizacion de Consumidores y Usuarios/OCU (Spanien) and Fédération Romande des consommateurs/FRC (Schweiz) (BEUC files complaint against TikTok for multiple EU consumer law breaches, www.beuc.eu 16.02.2021; Hahn, EU-Verbraucherschützer zeigen TikTok an wegen Schleichwerbung bei Kindern, www.heise.de 16.02.2021, Kurzlink: https://heise.de/-5056784).

Niederlande

Bußgeld gegen Booking.com wegen verspäteter Breach Notification

Die niederländische Datenschutzbehörde (Autoriteit Persoonsgegevens – AP) hat Booking.com eine Strafe in Höhe von 475.000 € auferlegt, weil das Portal zu spät einen Vorfall gemeldet hat. Kriminelle haben über die Seite Daten von 4.109 Kundinnen und Kunden abgegriffen. Zugang bekamen die Betrüger über die Konten von Mitarbeitern von 40 Hotels in den Vereinigten Arabischen Emiraten. Diese erreichten sie via „social engineering". Über die Zugänge der Hotelangestellten kamen die Betrüger an Daten von Gästen, die in den Hotels über Booking.com Zimmer gebucht hatten. Neben Namen, Adressen, Telefonnummern und Buchungsdetails konnten in 283 Fällen auch Kreditkarteninformationen eingesehen werden – bei 97 Karten sogar samt der Sicherheitsnummer. Zudem versuchten die Kriminellen mehr Kreditkartendaten zu bekommen, indem sie sich als Mitarbeiter der Hotels ausgaben und die Gäste per Mail oder Telefon kontaktierten.

Booking.com behauptete gegenüber der Presse, es habe keine unerlaubten Zugriffe direkt über die eigene Seite oder eigene Systeme gegeben. Der Vorfall sei zudem auf 40 Hotels beschränkt, bei denen Mitarbeiter ihre Zugangsdaten Kriminellen offenlegten. Gemäß der Bußgeldschrift gab es allerdings auch eine unbekannte dritte Partei, die auf das Booking.com-Extranet zugreifen konnte, in dem die Kundendaten hinterlegt waren. Zwar ist der unerlaubte Zugriff bereits 2019 geschehen, die Strafe folgte jedoch erst jetzt. 475.000 € muss das Portal zahlen, weil die Meldung des Vorfalls bei der Datenschutzbehörde erst 25 Tage, nachdem sie selbst davon wussten, erfolgte.

Gemäß der DSGVO müssen Datenlecks innerhalb von 72 Stunden nach Bekanntwerden gemeldet werden. Betroffene Kunden hatte man nach 22 Tagen informiert. Booking.com erklärt, man habe nicht so schnell reagiert, wie man hätte reagieren wollen. An einer Beschleunigung der Prozesse wird gearbeitet. Bei einem anderen Datenleck waren 2019 ebenfalls Kundeninformationen von Booking.com abgeflossen. Betroffen war dabei vor allem die französische Gekko Group (Weiß, Datenverlust zu spät gemeldet: Booking.com muss Strafe zahlen, www.heise.de 02.03.2021, Kurzlink: https://heise.de/-6004800).

Frankreich

Sensitive Labordaten im Web

Die illegale Verbreitung sensibler Patientendaten im Netz sorgt in Frankreich für Aufregung. Das auf Software im Gesundheitswesen spezialisierte Unternehmen Dedalus Frankreich stellte am 26.02.2021 einen „schwerwiegenden Akt von Cyberkriminalität" fest. Dieser hat demgemäß zur Verletzung der Daten von einigen Laborkunden geführt. Das Unternehmen habe 28 betroffene Labore in sechs verschiedenen Départements identifiziert. Man wolle die Quellen des Cyberangriffs ermitteln. Zuvor schon hatte es Berichte gegeben, wonach medizinische Daten von fast 500.000 französischen Bürgerinnen und Bürgern im Netz verbreitet worden seien. Die Datenschutzbehörde, die Nationale Kommission für Informatik und Freiheiten (CNIL), hatte daraufhin erklärt die Berichte zu prüfen, um offiziell zu bestätigen, dass eine entsprechende Datei zur Verfügung gestellt worden sei. Auch die Staatsanwaltschaft hatte eine Untersuchung eingeleitet. Bei den Daten

soll es sich Medien zufolge zum Beispiel um Angaben zur Blutgruppe, möglicher Schwangerschaft oder medikamentöser Behandlung der Laborkunden handeln. Die Daten sollen zwischen 2015 und 2020 gesammelt worden sein.

Zuvor hatte es u.a. Cyberangriffe auf zwei Krankenhäuser gegeben. Staatschef Emmanuel Macron hatte daraufhin angekündigt, eine Beobachtungsstelle für die Sicherheit von Gesundheitseinrichtungen schaffen zu wollen („Akt von Cyberkriminalität“ in Frankreich – Patientendaten aus Laboren im Netz, www.heise.de 27.02.2021, Kurzlink: https://heise.de/-5067272).

Schweiz

Volksabstimmung gegen privatisierte E-ID

Die Schweizer Stimmbürgerinnen und -bürger wollen gemäß dem Ergebnis einer Volksabstimmung Anfang März 2021 keine elektronische Identifikation (E-ID), die von privaten Anbietern herausgegeben und vom Staat lediglich kontrolliert wird. Sie haben dem vom Bundesrat ausgearbeiteten und vom Parlament verabschiedeten E-ID-Gesetz eine deutliche Abfuhr erteilt. Gemäß den Endresultaten aus den Kantonen erreichte das Bundesgesetz über die elektronischen Identifizierungsdienste (E-ID) nirgends eine Mehrheit. Unter dem Strich lehnten 64,4% der Abstimmenden die Vorlage ab. In absoluten Zahlen waren 1.777.100 Stimmbürger dagegen und nur 984.200 dafür. In zwanzig Kantonen liegt der Nein-Anteil zwischen 60 und 70%. In Basel-Stadt sowie in der Waadt wurde das E-ID-Gesetz mit 70,7% respektive 70,1% am klarsten verworfen. Im Tessin (55,8%), in Zug (59%) sowie in Nidwalden (59,6 Prozent) war das Nein etwas weniger deutlich.

Der Ball liegt nun wieder beim Bundesrat und beim Parlament. Selbst die Gegner des E-ID-Gesetzes wollen eine rasche Lösung. Umstritten war die Rollenteilung von Staat und Privaten. Das Stimmvolk sagte Nein zu einer privaten Lösung. Bei einer Neuauflage der E-ID wird also der Staat bei der Ausstellung und beim Betrieb federführend sein müssen. Im Abstimmungskampf hatte kaum jemand etwas grundsätzlich daran auszusetzen, die Digitalisierung voranzutreiben und die sichere Identifikation von Personen im Internet zu ermöglichen. Viele wünschen sich, dass im Internet einfacher Verträge abgeschlossen oder Behördengänge erledigt werden könnten. Kritisiert wurde nicht der Inhalt, sondern der Weg zum Ziel.

Das letztlich erfolgreiche Referendum gegen die Vorlage wurde von der Digitalen Gesellschaft lanciert und von SP, Grünen, Piratenpartei, VPOD, Internet Society Switzerland, Verein Public Beta, Grundrechte.ch sowie Seniorenorganisationen unterstützt. Auch der Gewerkschaftsbund (SGB), Travail Suisse, die GLP, die EDU und die Junge EVP engagierten sich für ein Nein zum E-ID-Gesetz. Es dürfe, so das Referendumskomitee, nicht sein, dass Daten in die Hände privater Firmen gelangten, die kommerzielle Interessen haben. Eine E-ID sei nur dann vertrauenswürdig, wenn sie staatlich sei. Der Bund müsse also selber eine E-ID anbieten und den Datenschutz gewährleisten. Gemäß dem gescheiterten Gesetz wären die Bundesbehörden lediglich für die Identifizierung einer Person zuständig gewesen.

Die unterlegenen Befürworter des E-ID-Gesetzes verwiesen dagegen auf die strengen Datenschutzvorschriften. Das Parlament habe den Datenschutz noch verstärkt. Auch der Eidgenössische Öffentlichkeits- und Datenschutzbeauftragte (EDÖB) setzte sich für die Vorlage ein, auch weil seine Rolle mit dem neuen Gesetz gestärkt worden wäre. Neu hätte eine staatliche Kommission für die Anerkennung der Aussteller von E-ID zuständig sein und diese auch beaufsichtigen sollen. Konkret hätten die Anbieter einer E-ID die Daten zur Person und Transaktion nicht zusammenführen oder für andere Zwecke verwenden dürfen. Zudem hätten die Transaktionsdaten nach sechs Monaten gelöscht werden müssen.

Eine gewisse Marktfreiheit für Anbieter sei gut und fördere den Innovationsgeist, hielten die Befürworter dagegen. Als Herausgeberin in den Startblöcken stand bereits die Swiss Sign Group, die die Swiss ID betreibt. Zum Konsortium gehören Post, SBB, Swisscom, Börsenbetreiber Six, Großbanken und Versicherungen. An die Stelle der Passbüros würden Unternehmen wie Banken und Versicherungen treten und die sensiblen Daten der Bürgerinnen und Bürger verwalten, warnten die Kritiker der Vorlage. Sie erachteten das Missbrauchspotenzial und die Risiken als zu groß, etwa bei einem Datendiebstahl. Eine elektronische Identität sei unumgänglich, wolle die Schweiz nicht ins Hintertreffen geraten, meinten die Befürworter. Sie verwiesen im Abstimmungskampf auch auf die Freiwilligkeit einer E-ID. Der Gang an den Schalter werde bei einem Ja nicht verunmöglicht. Nach dem Nein müssen sich auch die Digitalisierungsfreunde nun noch eine Weile damit abfinden (Beutler, Stimmvolk verwirft private E-ID wuchtig, herisau24.ch 07.03.2021).

Irland

Kritik an Datenschutzbeauftragter Dixon

Bei einer Anhörung im irischen Parlament zur europäischen Datenschutz-Grundverordnung (DSGVO) ist die Datenschutzbeauftragte des Landes mit Datenschutzaktivisten aneinander geraten. Der Österreicher Max Schrems forderte eine dringende Reform der Datenschutzbehörde des Landes, Johnny Ryan vom Irish Council for Civil Liberties (ICCL) beklagte gar, dass „systematische Grundrechtsverletzungen“ nicht überprüft würden. Die Datenschutzbeauftragte, Helen Dixon, wies die Kritik zurück und sprach von „übertriebenen“ und „vereinfachenden“ Vorwürfen. Die Anhörung im Justizausschuss war Teil einer für 2021 angesetzten Überprüfung der DSGVO in dem Land.

Bei der Durchsetzung der DSGVO kommt der irischen Datenschutzbehörde eine Schlüsselrolle zu, weil Internetkonzerne wie Facebook, Google und Twitter ihren europäischen Hauptsitz in dem Land haben. Deswegen ist die irische Data Protection Commission (DPC) für Datenschutzvorwürfe gegen diese zuständig, sie gilt aber als chronisch unterbesetzt und voreingenommen. In den von ihr eingeleiteten großen internationalen Verfahren kommt sie nur langsam voran und in den anderen Staaten, in denen die DSGVO gilt, wird die

Ungeduld und Unzufriedenheit immer größer. Zuletzt kam eine Aufforderung aus dem EU-Parlament die Ermittlungen zu beschleunigen.

Ryan erklärte den Parlamentariern, dass das Vorgehen der DPC Folgen für den Ruf und die Wirtschaft Irlands haben könnte. In 196 Verfahren, in denen die Behörde in den vergangenen drei Jahren die Führung übernommen habe, habe sie gerade einmal vier Entscheidungen getroffen. Die DPC sei also in 98% der Fälle, die von europaweiter Bedeutung sind, gescheitert. Schrems erklärte, die Verteidigung der DPC, dass sie nicht in jedem Fall zu einer Entscheidung kommen müsse, heiße, dass sie Beschwerden einfach im Papierkorb verschwinden lassen könne. Trotz über 10.000 Beschwerden im vergangenen Jahr plane die Behörde nur sechs bis sieben Entscheidungen, 99,93% landeten also im Papierkorb.

Dixon verwahrte sich gegen die Kritik und erinnerte daran, dass keine zwei Entscheidungen gleich seien. Beide Kritiker würden nur an der Oberfläche kratzen und teilweise übertreiben. Die Vorstellung, dass man absichtlich eine Regulierung verweigere, sei falsch. Ryan hatte etwa gefordert, ihr zwei weitere Datenschutzbeauftragte an die Seite zu stellen. Schrems hatte derweil daran erinnert, dass Dixons Kollegen und Kolleginnen in Spanien mit vergleichbaren Ressourcen zu fünf bis sechs Entscheidungen pro Tag kommen würden. In Österreich müssten Entscheidungen trotz des Geldmangels innerhalb von sechs Monaten entschieden werden (Holland, „DSGVO-Beschwerden in den Papierkorb“: Kritik an Irlands Datenschutzbeauftragter, www.heise,de 28.04.2021, Kurzlink: https://heise.de/-6030504).

Großbritannien

Gericht lässt anonyme Klage von Minderjährigen gegen TikTok zu

Ein 12-jähriges Mädchen aus Großbritannien hat das chinesische Kurzvideo-Unternehmen TikTok verklagt. Es wehrt sich dagegen, dass TikTok Informationen über Kinder sammle, die dazu verwendet werden, den Algorithmus der App zu verbessern und auf die Nutzerinnen und Nutzer zugeschnittene Inhalte auszuspielen. Dies verstoße gegen die geltenden Kinderschutzgesetze von Großbritannien, aber auch der EU. TikTok nutzt demnach die persönlichen Daten von Minderjährigen – insbesondere aber auch von Kindern unter 13 Jahren – dazu deren Verhaltensmuster und Vorlieben zu analysieren. Dies soll dazu führen, dass die Kinder die App häufiger und länger benutzen – obwohl die AGB der App klar festhalten, dass es unter-13-Jährigen nicht erlaubt ist, diese zu nutzen.

Die 12-Jährige wird bei ihrer Klage von Anne Longfield, der Beauftragen für Kinder in Großbritannien, unterstützt. Diese teilt die Meinung des Mädchens über die illegale Informationsbeschaffung der App. Longfield fordert von dem höchsten Gericht in England, dass alle Informationen, die TikTok über die 12-jährige Klägerin gesammelt hat, gelöscht werden müssen. Dies solle einen Präzedenzfall darstellen, der den Umgang des Unternehmens mit ähnlichen Informationen diktiert.

Bemerkenswert ist in dem Fall, dass das Gericht es der Klägerin erlaubt hat, die Klage anonym auszusprechen. Der Richter hat dies damit begründet, dass dem Mädchen möglicherweise Online-Mobbing von Seiten anderer Kinder oder Influencern droht, würde ihr Name bekannt gemacht werden: „Sie müsste mit wütenden Reaktionen von Personen rechnen, die ihren Status oder ihre Einkommensquelle bedroht sehen.“

Es ist nicht das erste Mal, dass TikTok sich mit solchen Vorwürfen auseinandersetzen muss. Bereits im Jahr 2019 musste das Unternehmen in den USA 5,7 Mio. Dollar Strafe bezahlen, weil es persönliche Informationen von Minderjährigen abspeicherte (DANA 3/2019, 165). Ein ähnliches Urteil wurde in Südkorea im Jahr 2020 gesprochen. Bei TikTok heißt es derweil: „Privatsphäre und Sicherheit stehen bei TikTok an erster Stelle und wir haben robuste Regelungen, Prozesse und Technologien im Einsatz, die alle Nutzerinnen und Nutzer und insbesondere die jungen schützen. Da wir nicht über diese Klage in Kenntnis gesetzt wurden, sind wir erst vom britischen Gericht darüber informiert worden. Nun sind wir daran die Implikationen zu überprüfen.“

Die AGB der App legen deutlich dar, dass es unter-13-Jährigen nicht erlaubt ist, den Service von TikTok zu benutzen und alle User, die einen Account erstellen, müssen ihr Alter angeben. Profile, die den Anschein haben, dass sie von Personen, die jünger als 13 Jahre alt sind, betrieben werden, werden von TikTok, so die Ansage, gelöscht (Zeier, 12-Jährige verklagt TikTok, www.20min.ch 04.01.2021).

Großbritannien

Kindergarten-Überwachungssystem war hackbar

Das in Großbritannien im Einsatz befindliche Überwachungskamerasystem für Kindergärten NurseryCam musste abgeschaltet werden, weil ein schweres Datenleck die Vertraulichkeit gefährdete, indem es die Anmeldeinformationen der teilnehmenden Eltern offen zugänglich machte.

NurseryCam erlaubt Eltern ihren Nachwuchs nach dem Absetzen dort aus der Ferne zu beobachten. Dazu nutzt es mehrere Kameras und einen digitalen Videorecorder (DVR). Zu diesem Zweck teilt die Firma hinter dem Überwachungssystem FootfallCam den Eltern Anmeldedaten mit. Eine Sicherheitslücke in dem System hat dazu geführt, dass sich offenbar beliebig Daten der elterlichen Konten auslesen ließen – darunter Nutzername, Passwort, Klarname und E-Mail-Adresse. Daraufhin hat das Unternehmen die Betroffenen informiert und seine Server zunächst abgeschaltet, bis das Problem behoben ist. Angeschlossen sind 40 Kindergärten in Großbritannien.

Die Firma NurseryCam war von einem Externen auf die Sicherheitslücke aufmerksam gemacht und aufgefordert worden die Sicherheit zu verbessern. Das Unternehmen teilte mit, die Person – offenbar ein gutgesinnter ‚White-Hat‘-Hacker – habe sich „verantwortungsbewusst“ verhalten und offenbar keinen Schaden mit den Daten anrichten wollen. Darüber hinaus glaubt das Unternehmen, dass weder Kindergartenkinder noch das Personal unerlaubt beobachtet worden seien. Das Abschalten der

Server nannte die Firma eine Vorsichtsmaßnahme.

Das Unternehmen hat zudem die britische Datenschutz-Aufsichtsbehörde (Information Commissioner's Office, ICO) über den Vorfall informiert. Firmen in Großbritannien sind verpflichtet, Datenschutzverletzungen von „erheblicher Auswirkung" binnen 24 Stunden an das ICO zu melden. Die Sicherheit des Kamerasystems war schon vorher anfällig gewesen. Über die zugehörige Mobil-App hatte sich jeder Administratorzugriff verschaffen und damit die Anmeldung als Nutzer umgehen können. Darauf soll das Unternehmen schon 2015 hingewiesen worden sein; es hatte die Entdeckung jedoch gemäß Presseangaben heruntergespielt und diese Lücke erst später geschlossen (Wittenhorst, Großbritannien: Kindergarten-Überwachungskameras wegen Datenleck abgeschaltet, www.heise.de 21.02.2021, Kurzlink: https://heise.de/-5061272).

Israel

Impfgesetz vorläufig nicht anwendbar

Das Oberste Gericht Israels legte mit einer einstweiligen Entscheidung am 10.03.2021 auf Antrag von Menschenrechtsgruppen ein Ende Februar vom Parlament beschlossenes Gesetz auf Eis, das die Weitergabe der Namen, Adressen und Telefonnummern von ungeimpften Israelis an lokale Ämter sowie an das Bildungs- und Sozialministerium erlaubt hätte. Dies hat zur Folge, dass die Betroffenen vorerst keinen direkten Druck der Behörden fürchten müssen. Ziel sollte laut dem Parlament sein, die Zögerlichen und Zweifler „persönlich zu ermutigen sich impfen zu lassen". Ins Visier genommen werden sollten auch diejenigen, die nach der ersten Dosis nicht zum zweiten Impftermin erschienen sind. Die Opposition hatte datenschutzrechtliche Bedenken gegen das Gesetz geäußert, blieb aber in der Minderheit.

Gerichtspräsidentin Esther Hayut begründete die Justizentscheidung damit, dass es in der Corona-Pandemie zu einer „fortschreitenden Erosion der Privatsphäre" komme. Die Regierung wurde aufgefordert noch einmal den genauen Nutzen des im Eiltempo beschlossenen Gesetzes zu erklären.

Die Datenweitergabe ist nicht der einzige Schritt, mit dem Israel bei der Pandemiebekämpfung auf Neuland vorzudringen versucht. So startete das Gesundheitsministerium ein Pilotprojekt mit einer sog. elektronischen Armfessel: 100 Menschen, die aus dem Ausland nach Israel zurückkehren, müssen diese in ihrer Heimquarantäne tragen, womit sie ständig lokalisiert werden können. Die Entscheidung dafür ist freiwillig – als Alternative droht allerdings die bisher für alle vorgesehene Hotel-Quarantäne in staatlicher Obhut. Das elektronische Armband war ein Jahr zuvor schon einmal diskutiert worden und damals als extreme Verletzung der persönlichen Rechte weithin zurückgewiesen worden. Im Laufe der Pandemie verändern sich offenbar die Maßstäbe: So meinte der israelische Rechtsexperte Adam Shenar, dass es bei Quarantäne in Sachen persönlicher Freiheit immer noch besser sei zu Hause ein Armband zu tragen als an einem fremden Ort eingesperrt zu werden (Impfgesetz in Israel kassiert, SZ 11.03.2021, 7; Münch, Impfdruck am Telefon, SZ 26.02.2021, 7).

Türkei

Einreiseverfahren wird digital

Seit dem 15.03.2021 fordert die Türkei von allen Einreisenden eine digitale Einreiseanmeldung. Demnach müssen Touristinnen und Touristen sowie andere Reisende binnen 72 Stunden vor der geplanten Einreise in die Türkei online ein Einreiseformular ausfüllen. Das digitale Einreiseformular wird auf der Website des türkischen Gesundheitsministeriums zur Verfügung gestellt. Dort haben Reisende beim Ausfüllen die Wahl zwischen mehreren Sprachen, neben Türkisch werden auch Deutsch, Englisch und Spanisch angeboten. Das Formular fragt ähnliche Daten ab, wie sie bisher von Einreisenden bei der Ankunft in einen Papiervordruck eingetragen werden mussten. Darunter sind Angaben zu Namen, Reisepassnummer und Kontaktdaten des Reisenden. Wie die Behörde im Begleittext erklärt, wird auf Basis dieser Daten automatisch ein persönlicher HES-Code erstellt. Er dient als Grundlage zur Nachverfolgung und Kontaktaufnahme, falls der Reisende während seines Aufenthaltes mit einer an COVID-19 erkrankten Person in Kontakt gekommen ist. Das Gesundheitsministerium erklärt, dass die erhobenen Daten ausschließlich den zuständigen Behörden mitgeteilt und sonst keinen Institutionen oder Personen zugänglich gemacht werden.

Der HES-Code wurde zuvor nur benötigt, wenn türkische Staatsbürger oder Touristen innerhalb der Türkei reisen und dabei beispielsweise Busse oder Inlandsflüge nutzen wollten. Nun wird er bereits vor der Einreise erstellt. Der Code ist entweder digital auf dem Smartphone oder in ausgedruckter Form mitzuführen und beim Check-in vorzulegen. Das türkische Gesundheitsministerium weist darauf hin, dass es auch an der Grenze zu Kontrollen des ausgefüllten Formulars kommen kann. Wurde es nicht eingereicht oder sind darin falsche Angaben enthalten, wird Urlaubern die Einreise in die Türkei unter Umständen verweigert.

Zusätzlich zum digitalen Einreiseformular benötigen alle Einreisenden in die Türkei ab sechs Jahren wie schon bisher einen negativen PCR-Test, der beim Abflug nicht älter als 72 Stunden sein darf. Urlauber aus Deutschland über zwei Jahren müssen darüber hinaus auch vor der Rückreise in die Bundesrepublik einen PCR-Test vornehmen lassen. Dieser darf frühestens 48 Stunden vor dem Heimflug erfolgen und wird noch vor Antritt der Heimreise durch die türkischen Behörden kontrolliert. Da die Türkei als Corona-Risikogebiet gilt, greift in Deutschland für Reiserückkehrer eine Quarantänepflicht (Türkei-Urlaub: Digitale Einreiseanmeldung ab 15. März Pflicht, urlaub.check24.de 11.03.2021).

USA

Überlegungen zur Beschränkung des internationalen Datentransfers

Der demokratische US-Senator Ron Wyden hat einen Entwurf für ein US-

amerikanisches Bundes-Datenschutzgesetz vorgestellt, das die Weitergabe persönlicher Informationen der US-Bürger ins Ausland wesentlich einschränken soll. Der „Protecting Americans' Data from Foreign Surveillance Act“ verknüpft dabei die Themen Nationale Sicherheit mit der Kritik an dem ausufernden Datenhandel. Wyden: „Zwielichtige Datenhändler sollten nicht dadurch reich werden, dass sie persönliche Daten von Amerikanern an Länder verkaufen, die unsere nationale Sicherheit bedrohen könnten.“

Das Gesetz sieht vor, dass die US-Regierung eine Liste von Ländern erstellt, an die ohne Probleme Daten geliefert werden können. Anbieter mit Sitz in einem anderen Land sollen sich erst um eine Exportlizenz bewerben müssen, bevor sie Daten von US-Bürgern verarbeiten dürfen. Zudem sollen Bürger Schadensersatzansprüche erhalten, wenn sie aufgrund solcher exportierter Daten Schaden erleiden oder gar im Ausland verhaftet werden.

Das Gesetz kombiniert mehrere aktuelle Strömungen in der Diskussion. Zum einen ist das Land besorgt um die chinesische Daten-Vormacht und versucht sich gegen den Einfluss chinesischer Anbieter abzuschotten. Zum anderen zeigen sich Wyden und Kollegen besorgt um das Ausmaß des Datenhandels von inländischen Firmen, die vor allem zu Werbezwecken Profile für jeden Internetnutzer anlegen und in einem komplexen Geflecht von Firmen und Lieferbeziehungen weitergeben. Wyden und mehrere Kollegen hatten von Firmen wie Google und Twitter, aber auch Providern wie AT&T und Verizon Auskunft gefordert, an welche Firmen Daten im Rahmen des sogenannten Real Time Biddings auf Werbeplattformen weitergegeben werden. Zwar hat der konkrete Gesetzentwurf kaum Chancen tatsächlich verabschiedet zu werden, doch mithilfe solcher Vorstöße wird die Diskussionsgrundlage für ein mögliches US-Datenschutzgesetz abgesteckt.

Johnny Ryan vom Irish Council on Civil Liberties (ICCL) vermutet, dass nicht nur geopolitische Gegner der USA so von dem globalen Datenstrom ausgeschlossen werden könnten. Er spekuliert in einem offenen Brief damit, dass Irland aufgrund der nachlässigen Bearbeitung von Datenschutzbeschwerden ebenfalls auf die Liste der unzuverlässigen Länder landen könnte. Dies habe enorme Konsequenzen: „Solche Lizenzen zu erlangen ist sehr schwierig – es werden die gleichen Anforderungen gestellt wie etwa für den Export von nuklearem Material.“ Um ein solches Szenario direkt zu verhindern, plädiert der ICCL für eine konsequentere Umsetzung der Datenschutz-Grundverordnung (Kleinz, USA: Gesetzentwurf soll Datenexport begrenzen – Sorge in Irland, www.heise.de 16.04.2021, Kurzlink: https://heise.de/-6018071).

USA

FISC rügt FBI-Auswertungen aus NSA-Massenüberwachung

Der Foreign Intelligence Surveillance Court (FISC) rügte erneut die nationale Polizei, das Federal Bureau of Investigation (FBI), weil es „im großen Stil“ Regeln zum Schutz der Privatsphäre von US-Bürgern verletzt. Dennoch billigte das unter strenger Geheimhaltung agierende US-Gericht die Anwendung der gesetzlichen Klausel im Foreign Intelligence Surveillance Act (FISA) für Massenüberwachung weiter. In einem mit Schwärzungen zur Veröffentlichung freigegebenen FISC-Urteil vom 18.11.2020 zählt der Vorsitzende Richter James Boasberg mehrere Fälle auf, in denen FBI-Agenten rechtswidrig nach Informationen über US-Amerikaner in E-Mails gesucht haben, die die National Security Agency (NSA) zuvor ohne individuelle Richtergenehmigungen erhoben hatte. Durch die neuen Beispiele untermauert der Richter ein schon wiederholt zutage getretenes Problem, das er bereits in früheren Entscheidungen angesprochen hatte.

Ein Mitarbeiter eines FBI-Außenbüros hat demnach von April bis Juli 2019 124 Abfragen unter Verwendung von Personenkennungen durchgeführt, die nicht den Standards entsprachen. Dabei handelte es sich z.B. um Personen, die bei der „Bürgerakademie“ des FBI mehr über die Rolle der Strafverfolgungsbehörden des Bundes lernen wollten. Dazu kamen Bürger, die in FBI-Dienststellen vorstellig wurden, um Reparaturen durchzuführen und Verbrechen anzuzeigen. Von August bis Oktober 2019 soll ein FBI-Arbeitsgruppenleiter in einem anderen Büro weitere 69 unzulässige Abfragen durchgeführt haben. Andere gemeldete Verstöße betrafen Fahnder, die es versäumten die Abfrage von FISA-Rohdaten für unzulässige Zwecke wie etwa Notrufabfragen zu beenden.

Das FBI soll versucht haben dem Problem Herr zu werden. Die Polizeibehörde wollte dazu gemäß Presseberichten neue Systemschutzmaßnahmen einführen und Mitarbeiter besser schulen. Die Coronavirus-Pandemie habe die Ermittler aber zunächst daran gehindert zu prüfen, ob der Ansatz greift. Trotzdem war Richter Boasberg bereit dem NSA-Überwachungsprogramm die gesetzlich vorgeschriebene Bestätigung zu erteilen, dass alles prinzipiell verfassungskonform ablaufe. Der Inlandsgeheimdienst kann die damit verknüpften Befugnisse also ein weiteres Jahr ausüben.

In dem Urteil geht es um Anordnungen nach Paragraf 702 FISA. Der zuletzt Anfang 2018 verlängerte einschlägige Artikel des Gesetzes zur Auslandsaufklärung erlaubt es der NSA von nationalen Unternehmen, Ämtern und Einrichtungen wie Telekommunikationsanbietern oder Bibliotheken E-Mails und andere Daten ihrer Kunden anzufordern. Die CIA, das National Counterterrorism Center und das FBI haben ebenfalls begrenzten Zugang zu den Informationsströmen. Das FBI erhält dabei Kopien abgefangener Nachrichten von und zu Zielpersonen, die es für laufende Ermittlungen zur nationalen Sicherheit als relevant erachtet. Das Volumen belaufe sich auf etwa 3,6% der Selektoren der NSA, erklärte ein leitender FBI-Beamter Medienvertretern am 26.04.2021. „Section 702“ FISA war zusammen mit Paragraf 215 des Patriot Acts, den der US-Kongress mit dem „USA Freedom Act“ bereits 2015 erstmals und 2020 erneut überarbeitete, mit den Snowden-Enthüllungen ins Licht der Öffentlichkeit gerückt. Die Klausel dient der NSA als Rechtsgrundlage für die weitreichenden Überwachungsprogramme Prism und Upstream, mit der sich der Geheimdienst massenhaft Daten von Internetfirmen beziehungsweise aus Glasfaserleitungen, darunter Unterseekabeln,

beschafft. Voraussetzung ist allein eine allgemeine Erlaubnis des FISC. Die NSA legte sich nach der öffentlichen Kritik zunächst selbst Schranken auf, die eine extreme Rundumüberwachung verhindern sollen (Krempl, Überwachung: US-Geheimgericht tadelt FBI erneut wegen schweren Missbrauchs, www.heise.de 29.04.2021, Kurzlink: https://heise.de/-6031350).

USA

Tesla-Bilder überführen Brandstifter

US-Strafverfolger sind offenbar auch dank der Kameras in einem Tesla auf die Spur eines mutmaßlichen Straftäters gekommen, der in Massachusetts eine Kirche angezündet und Reifen von mehreren Autos zerstochen haben soll. Gemäß einer eidesstattlichen Erklärung eines FBI-Agenten, in der die gesammelten Beweise zusammengefasst werden, konnten die Ermittler Fotos sicherstellen, die die Kameras des Elektroautos von dem Verdächtigen gemacht hätten, als der sich an den Reifen zu schaffen gemacht hat. Weil die Angriffe auf die Autos mit mutmaßlich gelegten Feuern in einer nahen Kirche in Zusammenhang gebracht werden, hätten die Fotos bei der Identifikation des Verdächtigen geholfen.

Bei den Ermittlungen geht es vor allem um die Zerstörung einer Kirche in Springfield (Massachusetts), die fast ausschließlich von Schwarzen besucht wurde. Die Ermittler gehen von einem Hassverbrechen aus, dem mehrere Versuche vorausgingen Brände in dem Gotteshaus zu legen. In Verbindung mit diesen Feuern seien auch Angriffe auf Autos in unmittelbarer Nähe der Kirche untersucht worden. Bei einem seien zwei Reifen eines Tesla gestohlen worden, der einen Farbigen als Besitzer habe. Die Ermittler konnten Fotos sicherstellen, die den Verdächtigen bei diesem Angriff zeigen. Die Überwachungsfotos des Teslas sind gemäß dem Bericht so gut, dass der Verdächtige darauf eindeutig identifiziert werden konnte.

Der Fall zeigt einmal mehr, wie viele Daten die Tesla-Fahrzeuge mit ihren Kameras und Sensoren sammeln können, nicht nur während der Fahrt. Die vom FBI verwendeten Fotos dürften im sogenannten Wächtermodus gemacht worden sein, in dem geparkte Teslas ihre Umgebung überwachen (DANA 4/2020, 227 ff.). Die chinesische Regierung hatte Ende März die Nutzung der Elektroautos durch Militärangehörige und Mitarbeiter wichtiger staatlicher Unternehmen eingeschränkt. Peking befürchtete Berichten zufolge, dass solche Daten bei einem Transfer in die USA an den Sitz des Herstellers die nationale Sicherheit Chinas gefährden könnten. Tesla-Chef Elon Musk hatte damals um Vertrauen in den verantwortungsvollen Umgang Teslas damit geworben (Holland, USA: Geparkter Tesla fotografiert mutmaßlichen Brandstifter, www.heise.de 16.04.2021, Kurzlink: https://heise.de/-6017816; siehe unten sowie in diesem Heft S. 116 und S. 131).

USA

Videosysteme bei Tesla, Polizei und Schulen geknackt

Unbefugte haben gemäß einem Medienbericht 150.000 Überwachungskameras einer US-Firma unter anderem in Krankenhäusern, Gefängnissen, Schulen und Polizeirevieren angezapft: Die Täter sollen das Passwort eines Super-Administrator-Zugangs im Internet gefunden haben. Der Betreiber der Kameras wirbt speziell mit Sicherheitsfeatures und Gesichtserkennung. Betroffen sind Unternehmen wie der Elektroauto-Hersteller Tesla und die IT-Sicherheitsfirma Cloudflare. Gemäß dem Bericht haben die Hacker Aufnahmen vom Tesla-Standort Shanghai vorgeführt. Das kalifornische Start-up Verkada, von dem die Kameras stammen, teilte in einer ersten Reaktion mit, man untersuche „das Ausmaß des potenziellen Problems".

Es passiert immer wieder, dass Bilder günstiger Sicherheitskameras für den Haushalt abgegriffen werden – vor allem wenn die Nutzer die voreingestellten Standard-Passwörter der Geräte nicht ändern. Dass eine Firma mit großen Kunden so leicht angreifbar ist, scheint bisher einzigartig. Die Eindringlinge haben den berichtenden Medienvertretern Aufnahmen der Videoüberwachungen aus einem Polizeirevier im US-Bundesstaat Massachusetts, einem Gefängnis in Alabama und einem Krankenhaus in Florida gezeigt. In dem Gefängnis sei es ihnen gelungen, 330 Kameras anzuzapfen. Bei Tesla seien es 222 Kameras gewesen. Sie hätten sich auch Zugang zum Videoarchiv der Verkada-Kunden verschafft. Nachdem Verkada kontaktiert worden war, hatten die Hacker den Zugang zu den Videosystemen verloren (Überwachungskameras bei Tesla, Polizei und Schulen geknackt, www.heise.de 10.03.2021, Kurzlink: https://heise.de/-5076211).

USA

Palantir-Aktie wenig erfolgreich

Seit der letzten Februar-Woche 2021 brachte die Palantir Technologies-Aktie den Anlegern kaum Freude. Der Kurs schwankte in New York um 25 US-Dollar, wobei unklar ist, wohin die Reise geht. In einem Interview erklärte CEO Alex Karp Ende März für das Unternehmen, einem Spezialisten für das Management großer Datenmengen, bestehe Entwicklungspotenzial vor allem im Bereich des Datenschutzes. Dafür müssten unbedingt Staat und Verwaltung aktiv werden, denn der Schutz sowohl der eigenen Daten, als auch der von fremden Daten überfordere Nutzer inzwischen massiv und sei nur noch von Software-Experten leistbar. Im zweiten Entwicklungsbereich, so Karp, gehe es um die Steuerung von militärischen Einrichtungen und die Verarbeitung von großen Mengen an Informationen. Hier wie dort setze Palantir auf fertige Softwarelösungen. Sie benötigten keine Software-Entwickler für die dauerhafte Anwendung und hätten daher einen hohen Nutzwert für die Kunden.

Einer der wichtigen Bereiche, in denen Palantir aktiv ist, ist die Bekämpfung von sexuellem Missbrauch von Kindern. Zur Verbrechensaufklärung und Vorbeugung arbeiten weltweit Behörden mit Palantir-Software. Das Unternehmen aus Palo Alto ist der WeProtect Global Alliance beigetreten. Die Or-

ganisation hat das Ziel, den Schutz von Kindern und Jugendlichen weiter zu verbessern. In der Alliance will Palantir auch Wege finden, um engere Kontakte zu anderen Mitgliedern wie Adobe und Unicef zu knüpfen.

Sicherheitsfragen, Datenschutz und medizinische Planungen haben Konjunktur. Große Unternehmen sind hier meist nicht selbst engagiert, sondern kaufen Software bei Zulieferern ein. Das bringt Mitbewerbern auch in Europa derzeit Aufschwung. Im Vergleich mit dem Index technischer Werte hat Palantir bislang in diesem Bereich nicht mithalten können (Scheibel, Palantir Technologies-Aktie: Viele Daten – wenig Power! www.finanztrends.de 21.03.2021).

China

Tesla-Autos für Funktionäre ungeeignet

Die chinesische Regierung schränkt gemäß Presseberichten die Nutzung von Tesla-Fahrzeugen durch Militärangehörige und Mitarbeiter wichtiger staatlicher Unternehmen ein. Die Staatsführung in Peking befürchtet demnach, dass die von den E-Autos etwa von Überwachungskameras und Sensoren gesammelten Daten bei einem Transfer in die USA an den Sitz des Herstellers die nationale Sicherheit Chinas gefährden könnten. Deshalb habe die Regierung einige nationale Behörden angewiesen ihre Mitarbeiter nicht mehr mit Teslas zur Arbeit fahren zu lassen. Die Rede ist auch von einem Verbot des Einsatzes der Wagen in Kasernen sowie in Wohnkomplexen mit Familien von Angestellten in sensiblen Industrien wie der Luft- und Raumfahrt und in der öffentlichen Verwaltung. Es sei zu befürchten, dass Tesla-Fahrzeuge ständig im Aufnahmemodus seien und verschiedene Daten einschließlich kurzer Videos aufzeichneten. Der Schritt folgt auf eine Sicherheitsüberprüfung einzelner Fahrzeuge des Autobauers im Auftrag der chinesischen Exekutive. Dabei habe sich bestätigt, dass sich über die erhobenen Messwerte leicht verfolgen lasse, wann, wie und wo die Wagen benutzt werden. Ausgelesen würden auch die Kontaktlisten von Mobiltelefonen, die mit den akkubetriebenen Autos synchronisiert sind.

Der chinesische Staatschef Xi Jinping will China zunehmend unabhängig von ausländischer Technologie machen. Parallel verschärft sich seit Monaten der Handelskrieg mit den USA. Laut den Berichten reagiert China mit der Anweisung auf US-Exportbeschränkungen für Komponenten für Kommunikationsgeräte chinesischer Unternehmen wie Huawei. Washington hat den Netzausrüster und Smartphone-Hersteller als Bedrohung für die nationale Sicherheit eingestuft und einen Bann für dessen Produkte in US-Mobilfunknetzen ausgesprochen. Der chinesische Markt ist für Tesla immer wichtiger geworden. Nicht zuletzt der Verkauf von 147.445 Fahrzeugen in dem Land verhalf dem E-Mobilitätsunternehmen 2020 zum Rekord von insgesamt rund 500.000 Fahrzeugauslieferungen weltweit. Nach der Eröffnung eines Werks in Schanghai setzte sich der Konzern 2020 als Marktführer für Elektroautos vor einheimischen Herstellern durch.

Elon Musk, Chef und „Technoking" von Tesla, warb angesichts der Vorwürfe um die Gunst der Chinesen: „Für uns ist der Ansporn groß mit Informationen sehr vertraulich umzugehen", betonte er am 20.03.2021 als virtueller Teilnehmer am Chinesischen Entwicklungsforum in Peking: „Sollte Tesla Autos benutzen, um in China oder anderswo zu spionieren, werden wir dichtgemacht." Es wäre gut, wenn China und die USA sich generell weniger argwöhnisch gegenüberstünden. Tesla hält sich nach eigenen Angaben mit seinen Datenschutzbestimmungen an chinesisches Recht.

Im Herbst 2020 war das Netzwerk Datenschutzexpertise in einem Gutachten zum Schluss gekommen, dass die Datenverarbeitung in einem Tesla 3 „in vieler Hinsicht gegen die europäischen Vorgaben" des Daten- und des Verbraucherschutzes verstößt. Acht Kameras gewährten eine 360-Grad-Rundumüberwachung der Fahrzeugumgebung in bis zu 250 Meter Entfernung. Ergänzt würden sie durch Ultraschall- und Radarsensoren. Tesla-Fahrzeuge dürften aufgrund des damit verknüpften Wächtermodus „auf europäischen Straßen nicht zugelassen werden". Die niederländische Autoriteit Persoonsgegevens hat als zuständige EU-Datenschutzaufsichtsbehörde Verfahren gegen den US-Konzern am Laufen, zu denen sie sich aber erst nach deren Abschluss äußern will. Das Bayerische Landesamt für Datenschutzaufsicht hatte angekündigt dem Wächtermodus rechtlich und technisch auf den Zahn fühlen zu wollen, war aufgrund von Corona-Beschränkungen aber bisher nicht dazu gekommen (Krempl, Datenschutzbedenken: China schränkt Tesla-Fahren für Funktionäre ein, www.heise.de 21.03.2021, Kurzlink: https://heise.de/-5993943, siehe oben S. 130).

China

Invasive Einreiseschikanen mit Corona-Gesundheitstests

Chinesische Behörden haben einen gesunden Deutschen nach dem Grenzübertritt über Wochen im Krankenhaus festgehalten, führten Dutzende medizinische Tests durch und hatten ihm hierfür immer wieder Blut abgenommen. Der Mann war Anfang 2021 nach China eingereist und hatte, wie vorgeschrieben, einen PCR- und einen IgA-Antikörpertest gemacht, die beide ohne Befund waren. Dass er zuvor an Corona erkrankt und wieder genesen war, hatte er in seinen Einreisedokumenten vermerkt.

Bei seiner Ankunft in China waren ein weiterer PCR- und der IgA-Test negativ. Der IgG-Test – ein weiterer Bluttest auf Antikörper – fiel dagegen positiv aus. Dies spricht dafür, dass der Mann die Infektion durchgemacht hat und nicht mehr ansteckend ist. Sowohl der PCR-Test als auch die Antikörper vom Typ IgA und IgM sind während der akuten Infektion und kurz danach positiv. Nach der Erkrankung fallen sie wieder negativ aus. Ein positiver IgG-Test ist dann eine erfreuliche Nachricht. Er zeigt an, dass Antikörper gegen Sars-CoV-2 vorhanden sind und Immunschutz besteht. Solange die Antikörper nachweisbar sind, ist es unwahrscheinlich, sich erneut anzustecken. Ein medizinischer Grund jemanden festzuhalten, besteht bei diesen Testergebnissen nicht.

Die chinesischen Behörden brachten den Mann dennoch in ein Krankenhaus, wo er sich nach einem Monat immer

noch aufhalten musste. Der Deutschen Botschaft wurde keine Einsicht in medizinische Unterlagen des Mannes gewährt, die erklären könnten, weshalb er festgehalten wird und wozu die Tests dienen sollten.

Der Fall ist nicht der einzige: Ein weiterer deutscher Staatsbürger wurde nach seiner Einreise in China trotz negativen Tests länger für Untersuchungen festgehalten. Ein entsprechender Fall wird aus einer europäischen Botschaft berichtet.

Auf diese Fälle hin hat das deutsche Auswärtige Amt am 09.02.2021 seine Reisehinweise in Bezug auf China verschärft: „Personen mit auskurierten Covid-19-Erkrankung werden, trotz negativer PCR- und IgM-Antikörpertests … bei Einreise in sofortige mehrwöchige Krankenhausquarantäne überführt und weitreichenden Untersuchungen unterzogen. Dies kann auch Personen betreffen, die aufgrund einer unentdeckten Erkrankung an Covid-19 noch Antikörper aufweisen.“ Das Gleiche könne auch für Personen gelten, die mit demselben Flug eingereist sind wie jemand, der im Anschluss positiv getestet wird: „Medizinische Maßnahmen der chinesischen Seite sind invasiv und beinhalten neben teils täglichen Blutentnahmen häufig auch Computertomografie-Aufnahmen.“ Aus wissenschaftlicher Sicht gibt es für dieses Vorgehen keine sinnvolle Erklärung.

Das Auswärtige Amt teilte mit, man habe bei der chinesischen Regierung Protest eingelegt. Untersuchungen gegen den Willen der Betroffenen sowie nicht sinnvolle Tests sehe man kritisch. Ebenso kritisiere man die langen Quarantänezeiten sowie die Hotelquarantäne. Maßnahmen müssten verhältnismäßig und medizinisch sinnvoll sein. Von den verschärften Einreisebedingungen in die Volksrepublik China seien auch Mitarbeiterinnen und Mitarbeiter des Auswärtigen Amtes und deren Angehörige betroffen: „Wir raten grundsätzlich von Reisen in die Volksrepublik China ab.“ Die Erfahrung zeigt, dass Einreisende neben Tests in Rachen und Nase auch Stuhltests unterzogen werden, in denen das Virus länger nachgewiesen werden kann.

Der Manager eines europäischen Konzerns bezeichnete einige der Maßnahmen als „durchgeknallt“. Jedes noch so unsinnige Verfahren werde genutzt, um bei Ausbrüchen später sagen zu können, dass man alles getan habe. Viele Beschäftigte schrecken aufgrund der Gruselgeschichten aus der Quarantäne und der Willkür bei ihrer Umsetzung inzwischen von einer Einreise oder einer Rückkehr nach China zurück. Infizierte Minderjährige werden bei der Einreise laut chinesischen Vorschriften von ihren Eltern getrennt und allein im Krankenhaus isoliert. Unabhängig vom Alter der Kinder ist es den Eltern verboten sie zu begleiten, so dass einige Kinder europäischen Diplomaten zufolge von ihren Eltern wochenlang getrennt waren. Das Auswärtige Amt bestätigt, dass man sich mehrfach gegen die Trennung von Eltern und Kinder gewehrt haben. Gemäß der deutschen Auslandshandelskammer sind die Einreisebeschränkungen inzwischen das größte Problem deutscher Firmen in China (Bartens/Deuber Festgehalten im Krankenhaus SZ 11.02.2021, 7).

Technik-Nachrichten

Tracking auch bei E-Mails

Das Nutzer-Tracking auf Webseiten ist seit Jahren ein großes Thema. Weitgehend unbeachtet blieb, dass es bei E-Mails kaum anders aussieht: Ein britischer E-Mail-Dienstleister hat analysiert, wie häufig so genannte Spy-Pixel in E-Mails zu finden sind. Die Ergebnisse sind in mancher Hinsicht überraschend: Wer seine Nachrichten nicht auf einer Web-Oberfläche im Browser liest, sondern im lokalen E-Mail-Client, ist demnach durch die bestehenden gesetzlichen Regelungen kaum geschützt.

Die eingebetteten Pixel lassen beim Absender unter anderem Schlüsse darüber zu, ob und wann eine E-Mail geöffnet wurde, wie oft der Nutzer sie angeschaut hat, welches Gerät beim Lesen der Nachricht genutzt wurde und von welcher IP-Adresse der Zugriff erfolgte – was in vielen Fällen Rückschlüsse auf den Standort des Users zulässt. Diese Datenerfassung wird von den Anbietern als ganz normales Mittel des Marketings angesehen. Sie verteidigen sich in der Regel damit, dass die Methoden irgendwo in den Nutzungsbedingungen oder Datenschutz-Vereinbarungen niedergeschrieben sind. Explizite Warnungen, wie sie Web-Nutzern inzwischen zwingend beim Einsatz von Cookies gegeben werden müssen, gibt es hier aber nicht.

Die Analyse zeigte, dass entsprechende Tracking-Pixel in etwa zwei Drittel aller E-Mails zu finden sind. Dieser Anteil ist ziemlich unabhängig davon, ob man den klassischen Spam mitzählt oder zuvor aussortiert. Und während quasi alle großen Marken freizügig auf diese Methode der Sammlung von Nutzerdaten zurückgreifen, verzichten am ehesten die großen Tech-Unternehmen auf ihren Einsatz. Das dürfte daran liegen, dass diese seit Jahren intensiv in die Auseinandersetzungen um den Datenschutz eingebunden und entsprechend vorsichtig sind.

Es gibt auch Fälle, die weit über das Tracking allgemeiner Informationen hinausgehen und bei den Usern für Unbehagen sorgen dürften. So erhielten Nutzende auch sehr explizite Nachfragen: „Ich habe gesehen, dass Sie meine E-Mail gestern gelesen, aber noch nicht geantwortet haben. Darf ich sie anrufen?“ Einen Schutz vor den kleinen Datensammlern gibt es bei E-Mails kaum. So lassen sich die meisten E-Mail-Clients nicht einfach mit Erweiterungen bestücken, die solche Tracking-Mittel ausfiltern. Und den Kampf darum, dass E-Mails auch im ganz klassischen Sinne als reiner Text empfangbar und lesbar sein sollten, haben selbst die meisten hartgesottenen User aufgegeben (Tracking in E-Mails: Hier läuft die Datensammlung unter dem Radar, 28.01.2021, winfuture.de/news121286.html).

Clubhouse setzt für Einladungen Adressbuchzugriff voraus

Seit dem Deutschlandstart des audiobasierten Social Networks Clubhouse hagelt es Kritik von Datenschützern. Ein häufiger Kritikpunkt: Wer jemanden auf die Plattform einladen will, der muss der App dazu Zugriff auf das eigene Adressbuch gewähren. Daraufhin sendet die App sämtliche dort erfassten Telefonnummern an die Betreiberfirma Alpha Exploration. Dass die übertragenden Telefonnummern gespeichert werden, zeigt sich in Clubhouse daran, dass die App zu jeder Telefonnummer aus dem eigenen Adressbuch sagen kann, wie viele „Freunde" sie bereits auf Clubhouse hat. Der Anbieter sammelt demnach Daten von Menschen, die selbst in keinem direkten Kontakt zu dem Dienst stehen und dessen Datenschutzrichtlinien nie widersprechen konnten.

Offenbar wird das Adressbuch nicht nur einmalig beim ersten Aufruf der App an die Clubhouse-Betreiber übertragen. Wie eine Datenanalyse von Zerforschung.org zeigt, werden die gespeicherten Telefonnummern bei jedem Aufruf der Einladefunktion erneut an einen Server des Anbieters gesendet. So könnte Alpha Exploration im Laufe der Zeit nachvollziehen, wer sich wann kennengelernt hat. Immerhin zeigt die Datenanalyse aber auch, dass wirklich nur die Telefonnummern und nicht auch die dazugehörigen Namen übertragen werden.

Wer möchte, der kann Clubhouse unter iOS auch nachträglich den Zugang zum Adressbuch entziehen. Dazu geht man zunächst auf „Einstellungen" und wählt dort den Eintrag „Datenschutz" aus. Unter „Kontakte" kann man dort Clubhouse den Zugang zum Adressbuch entziehen. Beim nächsten Aufruf der Einladefunktion von Clubhouse fragt die App dann erneut, ob Clubhouse die Kontakte übermittelt bekommen darf. Im Fall der Ablehnung kann man auch keine weiteren Menschen in die App einladen. Da Clubhouse seine Popularität in Teilen auch der künstlichen Verknappung von Zugängen verdankt, dürften die meisten Nutzerinnen und Nutzer diesen Weg aber wohl eher nicht wählen – zumindest nicht, solange sie noch Einladungen vergeben wollen (Clubhouse und Datenschutz: So fleißig sammelt die App eure Kontaktdaten, t3n.de 01.02.2021).

KI analysiert Genwirkmechanismen

Forschende kartografieren seit Jahren für viele Organismen die Positionen der Gene in der DNA, doch die Steuerung der Genaktivität ist noch wenig verstanden. An welchen Stellen ist kodiert, welche Gene ein Organismus wann in welchem Gewebe einsetzt und damit die gewebespezifischen Proteine herstellt? Ein interdisziplinäres Team aus Forschenden der TU München, des Stowers Institute for Medical Research in Kansas City und der kalifornischen Stanford University hat Teile dieser komplexen Regulierung in der DNA-Sequenz von Mäusen entdeckt. Mäuse gelten als Modellorganismus, dessen regulatorischen Konzepte den menschlichen ähneln. Ein speziell trainiertes neuronales Netzwerk spürte nun zuvor nicht verstandene Sequenzen auf.

Žiga Avsec, Doktorand im Team vom Professor Julien Gagneur in München, hat dafür in enger Zusammenarbeit mit Bioinformatikern aus Stanford ein neuronales Netzmodell entwickelt. Base Pair Network (BPNet) ist eine Variante der Convolutional Neural Networks, die vor allem Bilddaten analysieren. Neuronale Netze mit der BPNet-Technik verfolgen einen ähnlichen Bottom-up-Ansatz wie Systeme zur Gesichtserkennung. Diese erkennen Schicht für Schicht zunächst einfache Kanten und Linien, dann in höheren Schichten zusammenhängende Formen und schließlich komplexe Gesichter. Die Forscher entschieden sich, auf ähnliche Weise nach Motiven in den Basensequenzen der DNA zu suchen. Allein das Mäuse-Genom besteht aus 2,5 Milliarden Basenpaaren, beim Menschen sind es fast 3,3 Milliarden. Entscheidend für deren Wirkung ist nicht nur die Sequenz der entsprechenden vier Buchstaben (A, C, G und T für die beteiligten Basen Adenin, Cytosin, Guanin und Thymin), sondern vor allem die räumliche Anordnung der Basenpaare in der Spirale der DNA-Doppelhelix. Die übersetzten die Forscher in einfache Pixelmuster.

Gagneur erläutert: „Für diese Bilddaten stand uns dann das ganze Arsenal der KI-Bilderkenner zur Verfügung, um wiederkehrende Motive zu entdecken." Die gesuchten Motive sind Bindungsstellen für sogenannte Transkriptionsfaktoren (TF), Proteine, die die Aktivierung von Genen steuern. Ein TF findet sein Motiv, indem er dort exakt hineinpasst wie ein Schlüssel in sein Schloss. Das eingesetzte neuronale Netz umfasst, so Gagneur, elf Schichten und insgesamt nahezu 131.000 trainierbare Parameter. Diese Komplexität ermöglicht es Motive zu mehreren TF gleichzeitig zu suchen, um nicht nur der Verteilung einzelner Fragmente, sondern zugleich ihrem Zusammenspiel und der übergeordneten Syntax auf die Spur zu kommen. Allerdings meldete die KI zunächst nur das Vorhandensein der gesuchten Motive. Erst mit Methoden, die die Entscheidungswege der KI erklären, lässt sich, so Avsec, zeigen, an welchen Stellen der DNA die TF tatsächlich anbinden und wie diese Bindungsstellen konkret aussehen.

Als Trainingsdaten dienten 100.000 Abschnitte einer Mäuse-DNA mit jeweils etwa 1.000 Basenpaaren; insgesamt ein Datenvolumen von vier Gigabyte. Darin entdeckte die KI zu vier wichtigen TF neue Bindungsmotive. Man geht davon aus, dass im Mäuse-Genom noch wesentlich mehr Steuerelemente wirken. Für die menschliche DNA rechnen Forscher mit etwa 1.500 TF. Unterm Strich gelang es die Funktion der untersuchten TF zu ermitteln, beispielsweise bei der Selbsterneuerung von Stammzellen, die zugehörigen Motive mit der Genschere zu manipulieren und dadurch die KI-Vorhersagen experimentell zu bestätigen.

Die neuen Erkenntnisse sollen in zweierlei Hinsicht auf den Menschen übertragen werden: Zum einen erwarten die Wissenschaftler, dass sie Bindungsmotive wie in der Mäuse-DNA auch in anderen Organismen finden, insbesondere beim Menschen. Zum anderen ist die eingesetzte KI vielseitig und lässt sich auch für die Analyse menschlicher DNA trainieren. Diese Forschungsarbeiten laufen bereits. Künftig könnten die jüngst entdeckten Elemente der Genregulation helfen vererbbare Krankheiten besser zu verstehen und auch zu behandeln. Zudem ließen sich damit die Auswirkungen von Mutationen in einem Tumor einschätzen und

personalisierte Krebstherapien verbessern (Grävemeyer, Neuronale Netze entschlüsseln Code zur Genregulation, www.heise.de 21.03.2021, Kurzlink: https://heise.de/-5074686).

500 Mio. gescrapte LinkedIn-Profildaten zum Verkauf

In einem populären Hackerforum werden 500 Mio. LinkedIn-Profildaten zum Verkauf angeboten. Als Beweis können Interessierte zwei Mio. Datensätze für eine minimale Gebühr von 2 US-Dollar erlangen. Es handelt sich um öffentlich von den LinkedIn-Nutzern publizierte Daten wie Namen, E-Mail-Adressen, Telefonnummern und Arbeitgeber. LinkedIn untersuchte den Vorfall und bezeichnete ihn als unerlaubtes Scraping von Mitgliederdaten. Die kompletten 500 Mio. Profildaten können dann auf Anfrage für einen mindestens vierstelligen Preis erstanden werden. Sensible Daten wie Kennwörter, Kreditkarten- oder Bankinformationen gehören nach Ansicht der zum Beweis angebotenen Datensätze allerdings nicht dazu, da für die Datensammlung lediglich automatisierte Anfragen – sogenanntes „Scraping" – in großem Stil genutzt wurden.

Die angebotenen Mitgliederdaten umfassen LinkedIn-IDs, vollständige Namen, E-Mail-Adressen, Telefonnummen, Geschlecht, Berufsbezeichnung und andere Job-bezogene Daten, Links zu LinkedIn-Profilen und Profilen in anderen sozialen Netzwerken. Dies sind alles von den LinkedIn-Nutzern selbst veröffentlichte Daten und für andere Linkedin-Anwender einsehbar. Allerdings können sie für Phishing-Angriffe oder Brute-Force-Methoden zur Ermittlung von Kennwörtern genutzt werden.

LinkedIn erklärte: „Dieses sogenannte Scraping von Mitgliederdaten verstößt gegen die LinkedIn-Nutzungsbedingungen und wir arbeiten ständig daran unsere Mitglieder und ihre Daten zu schützen." Wenige Tage zuvor waren Daten hunderter Millionen Facebook-Nutzer im Netz in einem Forum für Cyberkriminelle veröffentlicht worden (s.u.). Im Jahre 2012 waren bereits LinkedIn-Passwörter im Umlauf. In einschlägigen Internet-Foren kursierte eine Liste mit über 6 Mio. Passwort-Hashes, die von LinkedIn stammen. 2016 wurde allerdings bekannt, dass das LinkedIn-Passwort-Leck desaströse Ausmaße angenommen hat, da nicht nur die damals veröffentlichten 6 Mio. Passwörter geklaut, sondern über 100 Mio. im Untergrund gehandelt wurden.

LinkedIn zählt nach eigenen Angaben derzeit fast 740 Mio. registrierte Nutzerinnen und Nutzer aus über 200 Ländern. Ob die 500 Mio. jetzt angebotenen Profildaten aktuell oder ein Resultat vorheriger Angriffe sind, ist noch unklar. Wer wissen will, ob sein LinkedIn-Profil betroffen ist, kann dies anhand einer Cybernews-Webseite und der bei LinkedIn hinterlegten E-Mail-Adresse überprüfen (Schräer, Linkedin: Daten von 500 Millionen Nutzern online zum Verkauf angeboten, www.heise.de 09.04.2021, Kurzlink: https://heise.de/-6009560).

Facebook-Daten erneut geleakt

Vertrauliche Daten mit Telefonnummern, E-Mail-Adressen und anderen Daten von hunderten Millionen Facebook-Nutzern sind Ende März 2021 in einem Forum für Cyberkriminelle aufgetaucht. Sie stammen aus einem Leak im Jahr 2019. Die IT-Sicherheitsfirma Hudson Rock hatte die Daten von 533 Millionen Facebook-Nutzern im Netz entdeckt – fast ein Fünftel aller Facebook-Nutzenden. Allein in Deutschland sind wohl sechs Millionen Menschen betroffen. Eine Sprecherin von Facebook erklärte: „Das sind alte Daten, über die bereits 2019 berichtet wurde. Wir haben das Problem im August 2019 entdeckt und behoben." Facebook hat nach jüngsten Angaben 2,8 Milliarden Nutzer, die mindestens einmal im Monat aktiv sind.

Die geleakten Daten umfassen den Facebook-Nutzernamen sowie den vollständigen Namen, die Telefonnummer, Geburtsdatum, Ort, biografische Angaben und in einigen Fällen auch die E-Mail-Adresse. Die Betroffenen stammen aus 106 Ländern und konnten anhand von Stichproben verifiziert werden. Betroffen ist u.a. auch unter „Nutzernummer 4": „Mark Zuckerberg: männlich: Palo Alto, Kalifornien" mit Telefonnummer und Beziehungsstatus. Auch wenn einige Informationen inzwischen veraltet sein dürften, enthält ein Datensatz dieser Größe dennoch genug aktuelles Material, um massenhaftes Phishing zu einer realen Gefahr werden zu lassen.

2019 waren Telefonnummern von 420 Millionen Nutzern im Netz aufgetaucht, nachdem eine Funktion zur Freundessuche für den Datenabgriff missbraucht worden war. Nun wurden die Daten für jeden verfügbar und mit geringen Programmierkenntnissen auswertbar. Die Telefonnummern waren zwar nicht offen sichtbar, konnten jedoch über automatisierte Anfragen – sogenanntes „Scraping" – in großem Stil abgerufen werden. Das verstieß gegen die Facebook-Regeln, war aber technisch möglich, bis das Online-Netzwerk die Funktion schließlich abschaltete. Sind solche Daten erst einmal im Umlauf, kann ihre Verbreitung im Netz kaum noch gestoppt werden. Scraping wurde für Facebook immer wieder zum Problem. So musste das Online-Netzwerk 2018 einräumen, dass vermutlich alle öffentlich zugänglichen Daten der damals bereits mehr als zwei Milliarden Nutzenden durch automatische Abrufe systematisch eingesammelt wurden. Die Zugriffe hatte Facebooks Entwickler-API gestattet, bis das Unternehmen diese Möglichkeit 2018 im Zuge des Cambridge-Analytica-Skandals unterband. Auch Hunderttausende deutsche Facebook-Nutzer waren betroffen. Allerdings gab es auch danach noch Lücken bei der Zugriffsbeschränkung, die sich einige Entwickler zunutze machten.

Später gab es Datenschutz-Debatten um die Firma Clearview AI, die öffentlich sichtbare Bilder unter anderem von Facebooks Foto-Plattform Instagram sammelte und auf dieser Basis eine Datenbank zur Gesichtserkennung zusammenstellte. Unter den Kunden von Clearview AI sind unter anderem US-Polizeibehörden (DANA 1/2020, 68; 2/2020, 125).

Die bekannte Leak-Website haveibeenpwned hat die Daten des Facebook-Lecks durchforstet und gut 2,5 Millionen Datensätze übernommen, in denen eine E-Mail-Adresse enthalten ist. Auf dieser Website können Benutzer anhand ihrer E-Mail-Adresse prüfen, ob ihre Daten in einem bekannt gewordenen Leak enthalten sind. Auch ein Freddy Greve hat sich ebenfalls mit diesem Leak be-

schäftigt und eigens eine Website eingerichtet, auf der Facebook-Nutzende prüfen können, ob ihr Nutzerkonto von dem Leck betroffen ist. Nach eigener Aussage hat Freddy Greve sämtliche Daten für Deutschland, Österreich und die Schweiz aus dem Leak eingepflegt – weitere Länder sollen folgen. Ist das eigene Facebook-Profil betroffen, zeigt die Website außerdem zu diesem Account die letzten fünf Ziffern der geleakten Mobilfunknummer an (Wittenhorst, Daten hunderter Millionen Facebook-Nutzer erneut im Netz entdeckt, www.heise.de 04.04.2021, Kurzlink: https://heise.de/-6005192, Brühl, Großes Datenleck bei Facebook, Zu wenig Schutz privater Daten, Daten von 533 Millionen Facebook-Nutzern geleakt, SZ 06.04.2021, 1, 4, 15).

Amazons Alexa-Apps mit Datenschutzproblemen

In einer Studie aus der North Carolina State University/USA wird eine Reihe von Datenschutzproblemen in Bezug auf die Apps dargestellt, mit denen Benutzer interagieren, wenn sie den Sprachassistenten von Amazon „Alexa" verwenden. Diese reichen von irreführenden Datenschutzrichtlinien bis hin zur Möglichkeit Dritter den Code ihrer Apps nach der Genehmigung durch Amazon zu ändern.

Anupam Das, Co-Autor des Artikels und Assistenzprofessor für Informatik, erläuterte: „Wenn Leute Alexa verwenden, um Spiele zu spielen oder nach Informationen zu suchen, denken sie oft, dass sie nur mit Amazon zu tun haben. Viele der Anwendungen, mit denen sie interagieren, wurden jedoch von Dritten erstellt, und wir haben im aktuellen Untersuchungsprozess mehrere Fehler festgestellt, die es Dritten ermöglichen, auf die persönlichen oder privaten Informationen der Benutzer zuzugreifen."

Die Probleme sind die auf Alexa verwendeten Apps, mit denen Benutzer alles tun können, vom Musikhören bis zum Einkaufen. Diese Anwendungen, die in etwa den Anwendungen auf einem Smartphone entsprechen, werden als Fertigkeiten (oder Fähigkeiten) bezeichnet. Amazon verkauft mindestens 100 Millionen Alexa-Geräte (möglicherweise doppelt so viel). Mehr als 100.000 Fertigkeiten stehen für Benutzer zur Auswahl. Da die meisten dieser Fertigkeiten von Drittentwicklern entwickelt werden und Alexa in Privathaushalten verwendet wird, wollten die Forscher mehr über potenzielle Sicherheit und Datenschutz erfahren.

Zu diesem Zweck verwendeten die Forscher ein automatisiertes Programm, um 90.194 einzigartige Fertigkeiten in sieben verschiedenen Fertigkeitengeschäften zu sammeln. Das Forschungsteam entwickelte außerdem einen automatisierten Überprüfungsprozess, der eine detaillierte Analyse jeder Fertigkeit bietet. Ein Problem, das die Forscher bemerkten, war, dass die Skill Stores den Entwickler anzeigen, der für die Veröffentlichung der Skill verantwortlich ist. Amazon überprüft nicht, ob der Name korrekt ist. Mit anderen Worten, ein Entwickler kann behaupten, jeder zu sein. Dies würde es einem Angreifer erleichtern sich unter dem Namen einer vertrauenswürdigeren Organisation zu registrieren. Dies kann wiederum dazu führen, dass Benutzer glauben, dass die Fertigkeit von der vertrauenswürdigen Organisation veröffentlicht wird, was Phishing-Angriffe ermöglicht.

Die Forscher fanden auch heraus, dass Amazon mehreren Fertigkeiten erlaubt, dieselbe Rufphrase zu verwenden, so Das: „Dies ist problematisch, denn wenn Sie glauben eine Fertigkeit zu aktivieren, aber eine andere aktivieren, besteht das Risiko, dass Sie Informationen an einen Entwickler weitergeben, an den Sie keine Informationen weitergeben wollten. Für einige Fähigkeiten ist beispielsweise ein Link zu einem Konto eines Drittanbieters erforderlich, z.B. zu einem E-Mail-, Bank- oder Social-Media-Konto. Dies kann ein erhebliches Datenschutz- oder Sicherheitsrisiko für Benutzer darstellen."

Darüber hinaus zeigten die Forscher, dass Entwickler den Code von Skills (im Amazon-Backend) ändern können, nachdem die Skills in den Läden platziert wurden. Die Forscher veröffentlichten speziell eine Fertigkeit und änderten den Code, um zusätzliche Informationen von Benutzern anzufordern, nachdem die Fertigkeit von Amazon genehmigt worden war. Das: „Wir haben uns nicht auf böswilliges Verhalten eingelassen, aber unsere Demonstration zeigt, dass es nicht genügend Kontrollen gibt, um zu verhindern, dass diese Sicherheitsanfälligkeit missbraucht wird."

Amazon verfügt über bestimmte Datenschutzbestimmungen, einschließlich expliziter Anforderungen in Bezug auf acht Arten personenbezogener Daten, u.a. Standortdaten, vollständiger Namen und Telefonnummern. Eine der Anforderungen ist, dass Fähigkeiten, die diese Daten anfordern, eine Datenschutzrichtlinie haben, die offen legt und erklärt, warum die Fähigkeit diese Daten wünscht und wie die Fähigkeit die Daten verwendet. Die Forscher stellten jedoch fest, dass 23,3% der 1.146 Fähigkeiten, die den Zugriff auf datenschutzrelevante Daten beantragten, keine Datenschutzrichtlinien hatten oder dass ihre Datenschutzrichtlinien irreführend oder unvollständig waren. Einige haben beispielsweise private Informationen angefordert, obwohl ihre Datenschutzrichtlinie behauptet, dass sie keine privaten Informationen anfordern.

Die Forscher geben auch unterschiedliche Empfehlungen, wie Alexa sicherer gemacht und Benutzer in die Lage versetzt werden können, fundiertere Entscheidungen über ihre Privatsphäre zu treffen. Die Forscher ermutigen Amazon beispielsweise die Identität von Skill-Entwicklern zu überprüfen und visuelle oder akustische Hinweise zu verwenden, um Benutzer darüber zu informieren, wenn sie Skills verwenden, die nicht von Amazon selbst entwickelt wurden.

Forscher Das: „Diese Studie ist nicht lang genug, um über alle Probleme oder Empfehlungen zu sprechen, die wir in dem Papier dargelegt haben. In diesem Bereich gibt es viel Raum für zukünftige Arbeiten. Zum Beispiel sind wir an den Erwartungen der Benutzer in Bezug auf Systemsicherheit und Datenschutz im Umgang mit Alexa interessiert." Das Papier „Hallo Alexa, ist diese Fähigkeit sicher? Sehen Sie sich das Alexa-Fähigkeits-Ökosystem genauer an" wurde auf dem Network and Distributed Systems Security Symposium 2021 vom 21. bis 24. Februar vorgestellt. Der Erstautor des Artikels ist Christopher Lentzsch von der Ruhr-Universität Bochum (Müller, Studie zeigt das Ausmaß von Datenschutzproblemen mit Amazon Alexa, kulturpoebel.de 07.03.2021).

Rechtsprechung

EuGH

Auch estnische Vorratsdatenspeicherung grundrechtswidrig

Der Europäische Gerichtshof (EuGH) hat auf Vorlage des estnischen Obersten Gerichtshofs, dem Riigikohus, mit Urteil vom 02.03.2021 entschieden, dass die Vorgaben zur Vorratsdatenspeicherung in Estland im Zusammenhang mit der dortigen Strafprozessordnung und einem Gesetz über die Staatsanwaltschaft gegen die in der EU verbrieften Grundrechte und die E-Privacy-Richtlinie verstoßen (Az.: C-746/18).

In Estland hatte ein Gericht eine Person wegen Diebstahls, Einsatz der Bankkarte eines Dritten und Gewalttaten gegenüber Beteiligten des Strafverfahrens zu zwei Jahren Gefängnis verurteilt. Die Staatsanwaltschaft hatte ihre Beweisführung unter anderem durch Zugriffe auf Verbindungs- und Standortdaten der Verdächtigen gestützt. Nachdem die Berufungsinstanz die Entscheidung bestätigt hatte, wandte sich die Betroffene an den Riigikohus. Der hegte Zweifel an der Vereinbarkeit der Voraussetzungen, auf deren Basis die Ermittler Zugang zu den auf Vorrat gespeicherten Daten hatten, mit dem EU-Recht.

Gemäß dem Urteil des EuGH erlaubt die Datenschutzrichtlinie für die elektronische Kommunikation Staatsbediensteten prinzipiell den Erhalt von Verkehrsdaten zur „Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten Zugang zu den von den Betreibern elektronischer Kommunikationsdienste gespeicherten“. Dabei sei der Eingriff in das Recht auf Privatheit der Betroffenen aber „in jedem Fall schwerwiegend“, solange Ermittler „genaue Schlüsse auf das Privatleben“ der Überwachten ziehen können.

Die damit verknüpfte besondere Tiefe des Grundrechtseingriffs ist unabhängig von der Länge des Zeitraums, für den der Zugang zu den genannten Daten begehrt wird, und von der Menge oder Art der verfügbaren Informationen. Ein Zugriff darauf müsse sich daher im Einklang mit dem Grundsatz der Verhältnismäßigkeit „auf Verfahren zur Bekämpfung schwerer Kriminalität oder zur Verhütung ernster Bedrohungen der öffentlichen Sicherheit beschränken“.

Eine ermittelnde und anklagende Staatsanwaltschaft ist gemäß der Entscheidung nicht in der Lage zu kontrollieren, ob die Voraussetzungen und Garantien für einen verhältnismäßigen Zugang zu den einschlägigen Daten inklusive eines wirksamen Schutzes vor Missbrauchsrisiken eingehalten werden. Diese Aufgabe könne nur ein Gericht oder eine vergleichbare unabhängige Stelle erfüllen. Auf die Staatsanwaltschaft, die in Estland das Verfahren leitete und die öffentliche Klage vertrat, treffe dies nicht zu.

Ob sich aus einer unzulässigen Datenbeschaffung ein Beweisverwertungsverbot ergibt, hat der EuGH dem vorlegenden Gericht zur Entscheidung überlassen, wobei das Recht auf ein faires Verfahren zu beachten ist. Relevant sei danach, ob die Beschuldigten „in der Lage sind sachgerecht zu den Informationen und Beweisen Stellung zu nehmen, die einem Bereich entstammen, in dem das Gericht nicht über Sachkenntnis verfügt, und geeignet sind die Würdigung der Tatsachen maßgeblich zu beeinflussen“.

Die Luxemburger Richter unterstrichen erneut, dass die E-Privacy-Richtlinie Rechtsvorschriften entgegensteht, die den Betreibern elektronischer Kommunikationsdienste „präventiv eine allgemeine und unterschiedslose“ Vorratsdatenspeicherung vorschreiben. Schon mehrfach hatte der EuGH zuvor umfassende, prinzipielle Vorgaben zum Aufbewahren der Telekommunikationsdaten auf Vorrat als unverhältnismäßig zurückgewiesen. In vier Fällen hielt das Gericht im Oktober 2020 aber Ausnahmen für möglich, wenn sich der betreffende Mitgliedstaat einer ernsthaften Bedrohung seiner nationalen Sicherheit gegenübersieht. Es stehe den EU-Ländern zudem offen „eine allgemeine und unterschiedslose Vorratsspeicherung von IP-Adressen vorzunehmen“. Bei den Internetkennungen seien die Grundrechtseingriffe weniger tief als etwa bei Standortdaten, aus denen sich Bewegungsprofile ableiten lassen (DANA 4/2020, 263 ff.).

Die Innenminister von Bund und Ländern forderten die Bundesregierung im Dezember 2020 auf „rechtssichere Handlungsmöglichkeiten“ für das Protokollieren von Nutzerspuren auszumachen. Das deutsche Gesetz zur mehrwöchigen Vorratsdatenspeicherung ist aufgrund von Entscheidungen von Verwaltungsgerichten weiterhin ausgesetzt. Es wird vom Bundesverfassungsgericht und dem EuGH überprüft. Der Wissenschaftliche Dienst des Bundestags geht davon aus, dass die Vorgaben nicht zu halten sind.

Auch die portugiesische Präsidentschaft des EU-Ministerrats hat die Vorratsdatenspeicherung wieder auf die Agenda gesetzt. Laut einem von der Bürgerrechtsorganisation Statewatch veröffentlichten, als vertraulich eingestuften Papier will die Ratsführung mit einer Umfrage an die Delegationen der Mitgliedsstaaten erkunden, welche Möglichkeiten diese vor allem für ein „selektives/gezieltes“ Sammeln insbesondere von IP-Adressen und Bestandsdaten von Nutzern sehen. Die Fragen gehen ins Detail, beziehen sich etwa auf Internetkennungen beim Ein- und Ausloggen sowie zu einem bestimmten Zeitpunkt einer Sitzung, den Einbezug auch von Zieladressen, statischen IP-Adressen sowie Portnummern. Ein Meinungsbild verschaffen wollen sich die Portugiesen zudem etwa darüber, ob „Over the Top“-Anbieter wie WhatsApp, Signal oder Skype einbezogen werden sollten. Darlegen sollen die EU-Länder, was sie als eine „angemessene“ Speicherfrist erachten. Der Rat hatte zunächst auf eine Studie der Kommission zur Vorratsdatenspeicherung gedrängt. Mit deren Ergebnis, wonach kein drin-

gender Handlungsbedarf besteht, ist er offenbar nicht zufrieden (Krempl, EuGH: Vorratsdatenspeicherung in Estland ist nicht mit EU-Recht vereinbar, www.heise.de 02.03.2021, Kurzlink: https://heise.de/-5069861).

Belgisches Verfassungsgericht

Gesetz zur TK-Vorratsdatenspeicherung wieder aufgehoben

Das belgische Verfassungsgericht hat am 22.04.2021 geurteilt, dass auch das 2016 verabschiedete zweite Gesetz zur einjährigen anlasslosen Vorratsspeicherung von Verbindungs- und Standortdaten im Bereich der Telekommunikation (TK) rechtswidrig ist, und hat damit die entsprechenden Bestimmungen aufgehoben (GVzNrn. 6590, 6597, 6599, 6601).

Bereits 2015 hatte das Verfassungsgericht die erste Fassung des Gesetzes gekippt, weil die Vorschriften unverhältnismäßig und die Schutzfunktionen nicht ausreichend seien. Das belgische Parlament hatte daraufhin einige Korrekturen eingefügt, im Kern aber an der Vorratsdatenspeicherung festgehalten. Das Gericht stellte nun fest, dass auch das neue Gesetz nicht mit dem EU-Recht vereinbar ist: „Die Pflicht zur Speicherung von Daten über die elektronische Kommunikation muss die Ausnahme sein und nicht die Regel.“ Eine solche Regelung sei allenfalls statthaft, wenn sie klaren Regeln hinsichtlich der Auswirkung und der Anwendung unterliege sowie Mindesterfordernisse aufstelle. Es sei zu gewährleisten, dass sich der Eingriff in die Grundrechte „auf das absolut Notwendige beschränkt“ und stets objektiven Kriterien genüge, „die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellen“.

Die belgischen Verfassungshüter orientieren sich dabei an den jüngsten Urteilen des Europäischen Gerichtshofs (EuGH) zu den nationalen Gesetzen zur Vorratsdatenspeicherung in Belgien, Frankreich und Großbritannien. Der EuGH hielt damit prinzipiell an seiner Linie fest, wonach umfassende, prinzipielle Vorgaben zum flächendeckenden Aufbewahren der Telekommunikationsdaten auf Vorrat als unverhältnismäßig gelten (DANA 4/2020, 263 ff.). Ausnahmen hielten die Luxemburger Richter für möglich, wenn sich ein Mitgliedstaat einer ernsthaften Bedrohung seiner nationalen Sicherheit gegenübersieht, die sich als tatsächlich und gegenwärtig oder vorhersehbar erweist. Dies könnte etwa bei Terrorangriffen der Fall sein. Den Beschlüssen zufolge steht es einem Mitgliedstaat auch offen unter strengen Auflagen „eine allgemeine und unterschiedslose Vorratsspeicherung von IP-Adressen vorzunehmen“.

Die Verfassungsrichter in Belgien kommen zu dem Schluss, dass das nationale Gesetz nicht einer der vom Gerichtshof beschriebenen Ausnahmen entspricht: „Es ist Sache des Gesetzgebers, Regelungen zu treffen, bei denen die in diesem Bereich geltenden Grundsätze im Lichte der Klarstellungen des Gerichtshofs beachtet werden.“ Bis dahin müsse das jeweils zuständige Strafgericht gegebenenfalls über die Zulässigkeit von Beweisen entscheiden, die nach den aufgehobenen Bestimmungen erhoben wurden.

Geklagt gegen die überarbeiteten Vorschriften hatten erneut unter anderem Belgiens Liga für Menschenrechte und die deutsch-französischsprachige Anwaltskammer Avocats.be. Das Gesetz war vor allem kritisiert worden, da es die Verwendung von auf Vorrat gespeicherten Daten zur Verfolgung von Straftaten erlaubte, „die mit einer einjährigen Haftstrafe geahndet werden können“. Dies hätte auf schwere Verbrechen und ernsthafte Bedrohungen der öffentlichen Sicherheit eingeschränkt sein müssen.

Avocats.be erinnerte den Gesetzgeber zudem an die vom EuGH betonte Gefahr, dass Berufsgeheimnisträger wie Rechtsanwälte, Ärzte, Abgeordnete oder Journalisten von der umstrittenen Form der Massenüberwachung in Belgien nicht ausgeschlossen worden seien. Damit könnten die Interessen etwa von Patienten oder Mandanten verletzt werden. Das belgische Justizministerium erklärte demnach bereits, dass es an einem erneuten „Reparaturgesetz“ arbeite.

In Frankreich hatte in der Woche zuvor der Conseil d'État (Staatsrat) das dortige Gesetz zur Vorratsdatenspeicherung zwar prinzipiell für rechtswidrig erklärt, aber schon gleich Hintertüren offen gelassen etwa zum Datensammeln für den Zweck der nationalen Sicherheit. Der Staatsrat genehmigte Strafverfolgern auch, auf die von Geheimdiensten gespeicherten Verbindungs- und Ortsinformationen zuzugreifen (Krempl, Belgisches Verfassungsgericht kippt Vorratsdatenspeicherung erneut, www.heise.de 27.04.2021, Kurzlink: https://heise.de/-2689182).

Conseil d´État (Frankreich)

Gericht akzeptiert Gesundheitsdaten-Hosting bei Amazon Web Services

Mit Beschluss vom 12.03.2021 stellte das oberste Gericht Frankreichs, der Conseil d´État, in einem vorläufigen Rechtsschutzverfahren fest, dass eine Auftragsverarbeitung für die Terminvergabe für Coronaimpfungen durch Doctolib mit der Fa. AWS Sarl in Luxemburg stattfinden kann. Mit Anträgen seit dem 26.02.2021 hatten medizinische und Bürgerrechts-Organisationen eine einstweilige Anordnung gegen das französische Gesundheitsministerium beantragt. Diesem sollte untersagt werden die Dienste der Fa. Doctolib bei der Durchführung des französischen Covid-19-Impfprogramms in Anspruch zu nehmen. Antragsteller waren folgende Verbände bzw. Personen: Association InterHop, Association Constances, Association Actions Traitement, Association les Actupiennes, Association Actup santé sud ouest, Syndicat de la Médecine générale(SMG), Union française pour une médecine libre (UFML), Syndicat national des jeunes médecins généralistes (SNJMG), Fédération des médecins de France (FMF), mehrere Einzelpersonen als Nutzender des Conseil de surveillance de l'AP-HP, Fédération SUD santé sociaux und Ligue des droits del' Homme. Ihren Antrag begründeten die Antragsteller damit, dass Doctolib Amazon Web Services (AWS) als Hoster nutzt und dadurch der Schutz der bei der Impfaktion erfassten Gesundheitsdaten nicht gewährleistet sei. Durch die Datenverarbeitung bei AWS hätten US-amerikanische Behörden gesetzlichen

Zugriff auf die sensitiven Impfdaten. Hierin läge ein Verstoß gegen die auch in Frankreich geltende DSGVO.

Der Conseil d´État stellte fest, dass die Auftragsverarbeitung für Doctolib mit der Fa. AWS Sarl, die ihren Sitz in Luxemburg hat, erfolgt, eine Tochter der US-amerikanischen Amazon Web Services Inc. Die Speicherung der im Auftrag verarbeiteten Daten erfolge in Frankreich und in Deutschland. Ein Datentransfer in die USA sei durch den Vertrag zwischen AWS und Doctolib nicht vorgesehen. Er bestätigt, dass eine Tochter von AWS auf der Grundlage von US-amerikanischen Regelungen (FISA, Executive Order 12333) verpflichtet werden kann, verarbeitete Daten herauszugeben.

Dies sei jedoch kein Grund, eine einstweilige Anordnung wegen der Terminvereinbarungen durch Doctolib zu erlassen. Hiervon erfasst würden keine „Gesundheitsdaten zu den möglichen medizinischen Gründen für eine Impfberechtigung“, sondern nur Daten zur Identifizierung der Betroffenen und zu Terminen und den Umstand der – altersunabhängigen – Impfberechtigung. Die Daten würden drei Monate nach dem Impftermin gelöscht. Die Daten seien bei AWS verschlüsselt gespeichert, wobei der Schlüssel in der Verfügungsmacht eines Treuhänders läge. Zudem bestehe die Möglichkeit für jeden Betroffenen durch Löschung seines Kontos seine Daten zu löschen. Angesichts dieser Garantien und der Sensitivität der Daten könne das Schutzniveau nicht als offensichtlich unangemessen bewertet werden (The urgent applications judge does not suspend the partnership between the Ministry of Health and Doctolib for the management of COVID-19 vaccination appointments, 12.03.2021, https://www.conseil-etat.fr).

BVerfG

Elektronische Fußfessel grundsätzlich verfassungskonform

Das Bundesverfassungsgericht (BVerfG) hat mit Beschluss vom 01.12.2020 entschieden, dass der Einsatz elektronischer Fußfesseln bei aus der Haft entlassenen Straftätern mit Rückfallrisiko mit dem Grundgesetz vereinbar ist (2 BvR 916/11, 2 BvR 636/12). Gemäß dem Zweiten Senat liegt in der sogenannten elektronischen Aufenthaltsüberwachung (elektronische Fußfessel) zwar ein „tiefgreifender Grundrechtseingriff insbesondere in das Recht auf informationelle Selbstbestimmung und das allgemeine Persönlichkeitsrecht“. Dieser Grundrechtseingriff sei aufgrund des Gewichts der geschützten Belange aber zumutbar und stehe nicht außer Verhältnis zu dem Gewicht der Rechtsgüter, wenn es um den Schutz vor „Straftaten gegen das Leben, die körperliche Unversehrtheit, die persönliche Freiheit oder die sexuelle Selbstbestimmung und Straftaten gegen die öffentliche Ordnung“ geht. Entscheidend ist, dass die Fußfessel nur angeordnet werden darf, wenn eine hinreichende Gefahr besteht, dass der Verurteilte weitere schwere Straftaten begeht.

Mit Verfassungsbeschwerden geklagt hatten zwei Männer, die von Gerichten in Rostock zum Tragen einer Fußfessel verpflichtet worden waren. Einer der Kläger war mehrfach wegen Vergewaltigung verurteilt worden. Der zweite hatte 1990 eine Frau ermordet und in Haft mehrfach mit Gewalt rebelliert. Wegen fortbestehender Gefährlichkeit wurde ihm bei seiner Entlassung 2011 eine Fußfessel angelegt. Die beiden Kläger hatten infrage gestellt, ob eine solche Maßnahme überhaupt mit dem Grundgesetz vereinbar ist.

Seit 2011 können Straftäter nach der Haft mit einer elektronischen Fußfessel rund um die Uhr überwacht werden. Einmal angelegt, lässt sich die Fessel von den Trägern nicht mehr öffnen. Über ein Satellitensignal ist ihr Aufenthaltsort jederzeit bestimmbar. Auf die Daten darf aber nur dann zugegriffen werden, wenn in der „Gemeinsamen elektronischen Überwachungsstelle der Länder“ (GÜL) in Hessen Alarm ausgelöst wird. Dort sind die Bewegungen der Träger auf einer Karte zu sehen. Bei einem Alarm wird bei dem Betroffenen angerufen, um zu prüfen, ob ein Fehler vorliegt – etwa ob der Akku der Fessel schwach ist.

Die Einführung der elektronischen Fußfessel hängt mit einer Entscheidung des Europäischen Gerichtshofs für Menschenrechte (EGMR) von 2009 zusammen. Der EGMR hatte geurteilt, dass die Sicherungsverwahrung in bestimmten Fällen gegen die Europäische Menschenrechtskonvention verstieß. Das BVerfG entschied nun dazu: „Das Urteil hatte zur Folge, dass Personen mit negativer Rückfallprognose in die Freiheit entlassen und sodann teilweise rund um die Uhr polizeilich überwacht wurden.“ Die Fußfessel sollte solche Überwachungsmaßnahmen ersetzen.

Die Straftäter, die nun geklagt hatten, waren nach langjährigen Freiheitsstrafen aus der Haft entlassen und polizeilich beobachtet worden. Dann war ihnen stattdessen die „elektronische Fußfessel“ angelegt worden. Ein zentraler Punkt in dem ausführlichen Beschluss des BVerfG ist die Frage, ob eine Datenüberwachung mit der Fußfessel gegen die Menschenwürde verstößt – das höchste Gut der Verfassung. Sie garantiert einen absolut geschützten „Kernbereich privater Lebensgestaltung“. In diesen Kernbereich dringt die Fußfessel aus Sicht des BVerfG nicht ein. Sie dient lediglich dazu, jederzeit den Aufenthaltsort des Betroffenen festzustellen: „In welcher Weise er sich an diesem Ort betätigt, ist nicht Gegenstand der Überwachung, da sein Handeln weder optischer noch akustischer Kontrolle unterliegt.“ Innerhalb der Wohnung sei eine genaue Ortung ausdrücklich untersagt.

Es findet also keine „Rundum-Überwachung“ statt und es wird kein lückenloses Persönlichkeitsprofil erstellt, das den Menschen bis in den letzten Winkel seiner Existenz ausleuchtet. Mit dieser Feststellung steckt der Senat zugleich die Grenzen künftiger technologischer Möglichkeiten ab: Ein Überwachungstool, das neben GPS-Daten gleich noch rund um die Uhr Bilder oder Töne mitlieferte, wäre voraussichtlich verfassungswidrig, selbst bei Überwachung besonders gefährlicher Straftäter. Die Verhältnismäßigkeit sei gegeben, wenn eine echte und erhebliche Gefahr unterbunden werden soll. Auch das Gebot der Resozialisierung sei nicht verletzt, weil mit dem leicht zu verbergenden Fußband niemand „sichtbar gebrandmarkt“ werde. Deshalb könne man nicht von einer Stigmatisierung sprechen. Die Wiedereingliederung in die Gesellschaft werde dadurch „nicht wesentlich erschwert“.

Seit 2017 können auch extremistische Täter überwacht werden. Außerdem darf das Bundeskriminalamt die Fußfessel bei sogenannten Gefährdern einsetzen, um Terroranschläge zu verhindern. Und auch die Polizeigesetze einiger Länder sehen einen solchen vorsorglichen Einsatz vor. In der aktuellen Entscheidung aus Karlsruhe geht es um den Einsatz bei Straftätern, die aus der Haft entlassen wurden. Einer Studie des hessischen Justizministeriums zufolge war die elektronische Fußfessel im Frühjahr 2020 deutschlandweit bei 122 Personen im Einsatz. Seit der Einführung der Maßnahme wurden mit ihr 269 Menschen überwacht. (Bundesverfassungsgericht: Elektronische Fußfesseln verstoßen nicht gegen das Grundgesetz, www.sueddeutsche.de 04.02.2021; Janisch, Bindendes Recht, SZ 05.02.2021, 6).

BGH

beA benötigt keine Ende-zu-Ende-Verschlüsselung

Der Bundesgerichtshof (BGH) folgt mit Urteil vom 22.03.2021 nicht der Ansicht von klagenden Anwälten, dass beim besonderen elektronischen Anwaltspostfach (beA) durchgehende Ende-zu-Ende-Verschlüsselt nötig sei (Az. AnwZ (Brfg) 2/20). Damit bestätigte der BGH ein Urteil des Berliner Anwaltsgerichtshofs von 2019, wonach der Bundesrechtsanwaltskammer (BRAK) ein Spielraum zugestanden wird, solange prinzipiell eine „sichere Kommunikation" gewährleistet ist.

Stein des Anstoßes in dem Fall ist die Besonderheit bei dem Anwaltspostfach, dass sich die darüber laufende Kommunikation unterwegs auf einem BRAK-Server mit einem Hardware-Sicherheitsmodul (HSM) „umschlüsseln" lässt. Damit wird die durchgehende Vertraulichkeitskette durchbrochen: Mit der Option zum zeitweiligen Ent- und späteren Wiederverschlüsseln ist ein Zugriff auf sensible Nachrichten innerhalb des HSM zumindest technisch prinzipiell möglich. Mehrere zugelassene Rechtsanwälte hatten zusammen mit der Gesellschaft für Freiheitsrechte (GFF) gegen diesen Ansatz geklagt. Sie drängten auf größere Sicherheit mithilfe einer durchgehenden Verschlüsselung. Die Karlsruher Richter erkannten zwar an, dass das beA nicht die Voraussetzungen einer Ende-zu-Ende-Verschlüsselung erfüllt. Das ändere aber nichts daran, dass die Nachrichten selbst zumindest während der Übertragung durchgehend verschlüsselt seien.

Es gebe keinen Anspruch auf eine noch weitergehende Sicherheitslösung, da die zuständige Verordnung nicht ausschließlich eine Ende-zu-Ende-Verschlüsselung vorschreibe. Es sei davon auszugehen, dass die gewählte Methode eine hinreichende Sicherheit gewährleisten kann. Die gesetzlichen Vorschriften seien mit einem zweistufigen Sicherheitscontainer erfüllt. Die BRAK muss die elektronischen Anwaltspostfächer laut der entsprechenden Verordnung auf Grundlage des Protokollstandards Online Services Computer Interface (OSCI) betreiben. Das beA sei als Drittprodukt am OSCI-Rechtsverkehr akzeptiert. Es verstoße auch nicht gegen die Grundrechte der Bürger dadurch, dass die beklagte BRAK keine Ende-zu-Ende-Verschlüsselung verwendet. Das anwaltliche Vertrauensverhältnis sei nicht gefährdet. Dem Beschluss zufolge gibt es auch keinen verfassungsrechtlichen Anspruch auf eine durchgehende Verschlüsselung. Die gewählte beA-Architektur sei sicher im Rechtssinne.

Die GFF zeigte sich enttäuscht von dem Urteil und sieht nun den Gesetzgeber gefordert. Dieser müsse eine Ende-zu-Ende-Verschlüsselung eindeutig vorschreiben. Das gebiete auch der verfassungsrechtliche Schutz des Mandatsgeheimnisses. Von der BRAK fordert die GFF einen Neustart, so der Vorsitzende Ulf Buermeyer: „Das beA war von Anfang an ein Sicherheits-Desaster. Außerdem ist das System sehr unkomfortabel und quälend langsam. Die BRAK sollte umgehend ein Update des Systems in Auftrag geben, das keine Hintertüren enthält und sich flüssig bedienen lässt." Der Mindeststandard einer Ende-zu-Ende-Verschlüsselung für sichere Kommunikation dürfe nicht ausgerechnet bei Anwälten unterschritten werden.

Die Bundesregierung hält das Entschlüsselungsrisiko indes „in Anbetracht der im Übrigen getroffenen Sicherheitsmaßnahmen" für akzeptabel. Eine Entschlüsselung von Nachrichten im laufenden Betrieb würde ein Zusammenspiel mehrerer Personen erfordern, da jeweils mehrere Mitarbeitende des Servicepartners und der BRAK beim Zusammenführen von Schlüssel und Botschaften gemeinsam agieren müssten. Das beA startete 2018 mit vielen sicherheitstechnischen Pannen, die Server mussten zeitweilig abgeschaltet werden. Eine Analyse der IT-Sicherheitsfirma Secunet verwies auf viele Sicherheitslücken, die laut der BRAK inzwischen abgedichtet sein sollen. Die Anwaltskammer hatte Anfang 2021 nach einer Klage auf Basis des Informationsfreiheitsgesetzes von FragDenStaat und der GFF Dutzende Dokumente zum beA herausgegeben, die Sicherheitsaudits, Resultate zu Penetrationstests und Verträge der Institution mit dem früheren Servicepartner Atos einschließen (Krempl, BGH: Kein Anspruch auf Ende-zu-Ende-Verschlüsselung beim Anwaltspostfach beA, www.heise.de 22.03.2021, Kurzlink: https://heise.de/-5995046).

BGH

AGB-Änderungen bedürfen der Kundenzustimmung

Der Bundesgerichtshof (BGH) hat in einem Grundsatzurteil vom 27.04.2021 zu schleichenden Vertragsänderungen und Gebührenerhöhungen gegenüber schweigenden Kunden den Spielraum für solche „Anpassungen" bei Banken zulasten ihrer Kunden deutlich verkleinert (Az. XI ZR 26/20). Der elfte Zivilsenat des BGH erklärte Klauseln der Postbank für unwirksam, nach denen eine Änderung der Allgemeinen Geschäftsbedingungen (AGB) und eben auch eine Anhebung der Entgelte schon dadurch wirksam werden, wenn der Kunde der geplanten Änderung nicht widerspricht. Nach der Vorstellung der Bank sollte es ausreichen, dass der Kunde „spätestens zwei Monate" vor einer Änderung der Konditionen darüber informiert wurde, gegebenenfalls elektronisch. Wenn ihm die Neuerung nicht passte, konnte er „fristlos und kostenfrei" kündigen.

Wenn er schwieg, wurde das als Zustimmung gewertet.

Nach den Worten des BGH-Vizepräsidenten Jürgen Ellenberger werden die Kunden durch solche Klauseln unangemessen benachteiligt. Denn dadurch sei nicht nur die Anpassung einzelner Details möglich. Die AGB seien vielmehr „ohne jede inhaltliche oder gegenständliche Beschränkung“ formuliert und ermöglichten damit „jede vertragliche Änderungsvereinbarung“. Den Kunden konnte durch bloße Bankeninformation – falls sie nicht widersprachen – ein ganz anderer Vertrag untergeschoben werden, etwa über ein Schließfach, das mit Kosten verbunden ist. Dies aber weicht, so der BGH, vom wesentlichen gesetzlichen Grundgedanken ab, wonach Schweigen grundsätzlich nicht als eine rechtsverbindliche Zustimmung gewertet werden darf.

Auch eine weitere Klausel, bei der es ausdrücklich um Entgelte geht, ist laut BGH nicht haltbar, da es dadurch zu Verschiebungen des Äquivalenzverhältnisses zwischen den Vertragspartnern kommen und damit zu einer Schwächung der Position des Kunden kommen könne. Solche Umgestaltungen der Beziehung zwischen Kunde und Bank könnten allein durch einen ausdrücklichen Änderungsvertrag vereinbart werden.

Das Urteil dürfte weitreichende Auswirkungen haben. Der BGH wies ausdrücklich darauf hin, dass die beanstandeten Klauseln im Wesentlichen den Musterbedingungen von Banken und Sparkassen entsprächen, also in der Branche (auch bei Änderungen zum Datenschutz, Red.) üblich sind. Die Kreditinstitute werden nun vermutlich versuchen, ihre Bedingungen der neuen Rechtsprechung anzupassen.

Ellenberger wollte bei der Urteilsverkündung nicht ausschließen, dass auch künftig Vertragsbedingungen zulässig sein können, die den fehlenden Widerspruch von Kunden als Zustimmung werten, etwa, wenn eine Anpassung an Gesetzesänderungen notwendig sei. Allerdings wird dies in deutlich geringerem Umfang erlaubt sein als bisher. Daran ändert auch die Tatsache nichts, dass § 675g des Bürgerlichen Gesetzbuchs eine solche Zustimmungsfiktion ausdrücklich vorsieht, freilich beschränkt auf „Zahlungsdienste“ wie das normale Girokonto. Ellenberger stellte klar, dass in solchen Fällen eine volle „Inhaltskontrolle“ der Klauseln stattfinde – also eine gerichtliche Prüfung, ob der Kunde unangemessen benachteiligt werde (Janisch, Um Antwort wird gebeten, SZ 28.04.2021, 17).

BGH-Ermittlungsrichter

Scheuer-Logfiledaten für Untersuchungsausschuss kein Tabu

Mit Beschluss vom 29.01.2021 entschied ein Ermittlungsrichter des Bundesgerichtshofs (BGH) auf Antrag der Bundestagsfraktionen von FDP, Linken und Grünen, dass die sogenannten Logfiles des Abgeordneten-Mail-Accounts von Andreas Scheuer im Rahmen der Ermittlungen des Maut-Untersuchungsausschusses ausgewertet werden dürfen. Aus den Logfiles lässt sich erkennen, wann, mit wem und mit welchem Betreff der Minister über diesen Account Mails ausgetauscht hat. Es geht um Kommunikation mit Staatssekretären oder Abteilungsleitern.

Die Opposition hatte Scheuer zuvor vorgeworfen, wichtige Maut-Mails, die vor allem über sein Abgeordneten-Postfach liefen, weiter geheim zu halten. Scheuer bestreitet das. Der Verkehrsminister hatte allerdings anfangs auch bestritten, dass überhaupt Maut-E-Mails über diesen Account liefen, und musste später zurückrudern. Sein Ministerium lieferte Dokumente an den Ausschuss nach und machte dafür ein „Büroversehen“ verantwortlich. Die Opposition vermutete, dass immer noch nicht alle Mails vorliegen.

Der Beschluss des BGH ist unangenehm für Scheuer. Er ist aber auch eine Ohrfeige für Unions- und SPD-Fraktion im Maut-Ausschuss, die es unter Verweis auf einen unzulässigen Eingriff ins Fernmeldegeheimnis abgelehnt hatten, den von der Opposition geforderten Zugriff auf die Daten Scheuers auch nur zu beantragen. Der BGH entschied nun jedoch, dass der Untersuchungsausschuss zu dem Antrag „verpflichtet“ sei. Er müsse den Bundestagspräsidenten zur Aufklärung um Vorlage dieser Logfiles bitten. Die Opposition habe schließlich konkrete Anhaltspunkte vorgetragen, die Zweifel an der Vollständigkeit der Minister-Mails begründeten.

Die Entscheidung dürfte außer in Scheuers Ressort auch in weiteren Ministerien für Unruhe sorgen, denn sie zeigt, dass der BGH die Rechte des Parlaments bei der Kontrolle von Ministern sehr hoch hängt. Der Schutz der Daten sei vor allem für Bürger gegen Eingriffe des Staates gedacht, auch Amtsträger könnten sich darauf berufen. Allerdings dürfe das nicht dazu führen, dass sie sich der Kontrolle durch das Parlament entziehen.

So seien Amtsträger verpflichtet, Privates und Dienstliches zu trennen. Auf Smartphones sei das auch für Minister technisch problemlos möglich. Die Logik des BGH: Wer nicht sauber trennt, muss damit rechnen, dass seine Kommunikation kontrolliert wird. Sonst könnten sich Minister schon dadurch der Kontrolle entziehen, dass sie Privates in Dienstliches einflechten. Das Gleiche gelte für Mails, die Minister-Angelegenheiten betreffen, aber über deren Bundestags-Account liefen. Der hohe Schutz der Abgeordneten-Kommunikation könne dann nicht zur Geltung kommen.

Die Opposition drohte mit einer Verlängerung des Maut-Ausschusses, wenn sich ihr Verdacht erhärtet. Dessen Ermittlungen waren am Tag vor dem Beschluss mit der Einvernahme von Scheuer eigentlich abgeschlossen worden. Falls die Analyse der Logfiles Ungereimtheiten ergebe, sei es, so FDP-Obmann Christian Jung, denkbar, „dass weitere Zeugen geladen werden müssen“ und der Abschlussbericht des Ausschusses erst im September fertig werde (Balser, Daten, die Scheuer gefährlich werden könnten, SZ 01.02.2021, 5).

OVG Schleswig-Holstein

Videoüberwachung bei Online-Prüfung ist zulässig

Das Schleswig-Holsteinische Oberverwaltungsgericht (OVG) lehnte mit unanfechtbarem Beschluss vom 03.03.2021 den Antrag eines Studierenden der Christian-Albrechts-Universität zu Kiel (CAU) ab eine entsprechende Satzungs-

regelung der CAU vorläufig außer Vollzug zu setzen, die ihn verpflichtet eine in elektronischer Form abzulegende Prüfung mit Videoaufsicht zu erdulden (Az. 3 MR 7/21).

Das OVG ließ den Antrag schon an der Zulässigkeit scheitern, weil der Antragsteller sein Ziel auf diesem Wege nicht erreichen und seine Rechtsstellung folglich nicht verbessern könne. Es sei davon auszugehen, dass die CAU davon abgesehen hätte überhaupt Prüfungen in elektronischer Form vorzusehen, wenn sie diese nicht an eine Videoaufsicht koppeln dürfte. Dies wiederum habe zur Folge, dass der Antragsteller im Falle eines gerichtlichen Erfolges überhaupt keine Prüfung ablegen könne, weil die alternativ anzubietenden Präsenzprüfungen nach der Hochschulen-Coronaverordnung des Landes grundsätzlich noch zu verschieben seien.

Im Übrigen hätte, so das OVG, der Antrag auch in der Sache keinen Erfolg gehabt, da die angegriffene Satzungsregelung über die Videoaufsicht auch unter Beachtung höherrangigen Rechts voraussichtlich rechtmäßig sei. Das Recht auf Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) sei nicht betroffen, da dieses nur vor einem (digitalen) „Eindringen" in die Wohnung schütze. Die Videoaufsicht erfolge jedoch nicht gegen den Willen der Studierenden. Sie könnten frei entscheiden, ob sie an der elektronischen Prüfung teilnähmen mit der Folge, Kamera und Mikrofon ihres Computers für die Aufsicht zu aktivieren, oder ob sie später eine Präsenzprüfung ablegten. Obwohl diese derzeit nicht durchgeführt werden dürften, sei die Freiwilligkeit ihrer Entscheidung ausreichend gesichert.

Der mit der Videoaufsicht verbundene Eingriff in das Grundrecht auf informationelle Selbstbestimmung sei durch das Gebot der Chancengleichheit gerechtfertigt. Danach müsse sichergestellt sein, dass bei einer Prüfung, für die keine Hilfsmittel zugelassen seien, eine Aufsicht unabhängig von der Prüfungsform stattfinden könne. Zur Erreichung dieses Zwecks sei die Videoaufsicht auch hinreichend geeignet. Dass sie zur Vermeidung von Täuschungshandlungen tatsächlich weniger geeignet sein könne als eine Aufsicht im Rahmen einer Präsenzklausur, weil der Bildschirm des Prüflings nicht einsehbar sei und sich außerhalb des Kamerawinkels unzulässige Hilfsmittel befinden könnten, schade nicht. Auch bei Präsenzklausuren ließen sich nicht sämtliche Täuschungsversuche verhindern. Mit technischen Problemen, die zu einem regelhaften Ausfall elektronischer Prüfungen samt Aufsicht führten, sei nach zwischenzeitlicher Etablierung der Videokonferenztechnik gerade im Bildungsbereich nicht mehr zu rechnen. Im Übrigen sei vorgesehen, dass die Prüfung bei technischer Undurchführbarkeit vorzeitig beendet werde und der Prüfungsversuch als nicht unternommen gelte. Gleichermaßen geeignete Alternativen gebe es gegenwärtig nicht. Schließlich sei die Regelung bei Abwägung der widerstreitenden Belange auch angemessen. Die Videoaufsicht führe gegenüber der Präsenzaufsicht zwar zu einer intensiveren Belastung, doch sei die Teilnahme an der elektronischen Fernprüfung freiwillig und die Freiwilligkeit ausreichend sichergestellt. Zu einem „unbeobachtbaren Beobachtetwerden" komme es nicht. Anders als etwa bei der Vorratsdatenspeicherung liege eine Überwachung von Prüfungen in der Natur der Sache und sei den Betroffenen bekannt.

Schließlich seien die Voraussetzungen und der Umfang der Datenerhebung und -verarbeitung in der Satzung der CAU hinreichend klar geregelt. Einer Regelung durch den Gesetzgeber habe es nicht bedurft, da er während der Corona-Pandemie bereits die entsprechenden Rechtsgrundlagen im Hochschulgesetz geschaffen habe (Corona – Videoaufsicht bei elektronischer Hochschulprüfung zulässig, www.schleswig-holstein.de 04.03.2021).

OVG NRW

Videoprüfungen sind vorläufig DSGVO-konform

Auch das Oberverwaltungsgericht Nordrhein-Westfalen (OVG NRW) hat mit unanfechtbarem Beschluss vom 04.03.2021 den Normenkontroll-Eilantrag eines Studenten aus Bonn abgelehnt, der sich gegen die Corona-Prüfungsordnung der Fernuniversität Hagen gewandt hatte (14 B 278/21.NE). Die Fernuni sieht in ihrer Corona-Prüfungsordnung als alternative Möglichkeit neben Präsenzprüfungen, die bisher durchgeführt wurden, videobeaufsichtigte häusliche Klausurprüfungen vor. Danach werden die Prüflinge durch prüfungsaufsichtsführende Personen über eine Video- und Tonverbindung während der Prüfung beaufsichtigt. Die Video- und Tonverbindung sowie die Bildschirmansicht des Monitors werden vom Beginn bis zum Ende der Prüfung aufgezeichnet und gespeichert. Die Prüfungsaufzeichnung wird nach dem Ende der Prüfung gelöscht. Dies gilt nicht, wenn die Aufsicht Unregelmäßigkeiten im Prüfungsprotokoll vermerkt hat oder der Student eine Sichtung der Aufnahme durch den Prüfungsausschuss beantragt. In diesem Fall erfolgt die Löschung der Aufzeichnung erst nach Abschluss des Rechtsbehelfsverfahrens. Mit dem Eilantrag begehrte ein Student, der an einer solchen Prüfung am 08.03.2021 teilnehmen wollte, die vorläufige Untersagung der Aufzeichnung und Speicherung der Daten, nicht aber des Filmens an sich. Er machte geltend, das Vorgehen verstoße gegen die Datenschutz-Grundverordnung und sein Recht auf informationelle Selbstbestimmung.

Das OVG begründete seine Ablehnung damit, dass die Rechtmäßigkeit der Aufzeichnung und Speicherung im Eilverfahren nicht geklärt werden könne. Die Datenschutz-Grundverordnung (DSGVO) lasse eine Datenverarbeitung zu, wenn sie für die Wahrnehmung einer Aufgabe erforderlich sei, die im öffentlichen Interesse liege oder in Ausübung öffentlicher Gewalt erfolge, die dem Verantwortlichen übertragen worden ist. Hochschulen seien zur Durchführung von Prüfungen verpflichtet. In Wahrnehmung dieser Aufgabe habe die Fernuniversität dem prüfungsrechtlichen Grundsatz der Chancengleichheit Geltung zu verschaffen. Dieser verlange, dass für vergleichbare Prüflinge so weit wie möglich vergleichbare Prüfungsbedingungen gälten, um allen Teilnehmern gleiche Erfolgschancen zu bieten. Insbesondere sei zu verhindern, dass einzelne Prüflinge sich durch eine Täuschung über Prüfungsleistungen einen Chancenvorteil gegenüber den rechtstreuen Prüflingen verschaffen.

Die Aufzeichnung und vorübergehende Speicherung dürfte sich im Ergebnis im Hinblick darauf, die teilnehmenden Prüflinge von Täuschungsversuchen abzuhalten, und im Hinblick auf ein sich im Verlauf der Prüfung ergebendes Bedürfnis nach Beweissicherung in der Sphäre des Prüflings, auch für eine vom Prüfling geltend gemachte Störung des ordnungsgemäßen Prüfungsablaufs, als geeignet und erforderlich erweisen. Die wegen der verbleibenden Rechtmäßigkeitszweifel erforderliche ergänzende Folgenabwägung falle zu Lasten des Antragstellers aus, da die durch die Aufzeichnung und Speicherung der Daten eintretenden Belastungen zumutbar seien (Oberverwaltungsgericht für das Land Nordrhein-Westfalen: Eilantrag gegen videoüberwachte Prüfung der Fernuniversität Hagen erfolglos, www.justiz.nrw 04.03.2021).

VG Wiesbaden

Löschbegehren muss in jedem Einzelfall geprüft werden

Das Verwaltungsgericht Wiesbaden (VG) stellte mit Beschluss vom 11.01.2021 ein Klageverfahren gegen den Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI) wegen Erledigung ein, in dem es um dessen Bescheid ging, der die Schufa nicht dazu verpflichtete einen negativen Eintrag zu löschen (Az.: 6 K 1045/20). Die Klage war erforderlich geworden, da der Betroffene mit seinem Antrag auf Löschung bei der Schufa und der anschließenden Beschwerde über die Weigerung der Schufa beim Hessischen Beauftragten für Datenschutz und Informationsfreiheit auf taube Ohren gestoßen war. Das Klagebegehren war darauf gerichtet, dass die ursprünglichen Bescheide aufgehoben und die Aufsichtsbehörde angewiesen wird eine Löschung der Negativeinträge bei der Schufa anzuordnen.

Bei einem parallelen Verfahren hatte eine Klägerin im Mai 2020 verwundert feststellen müssen, dass für sie ein Negativeintrag in Höhe von 110 Euro bestand. Der Eintrag bezog sich auf eine Forderung, die Ende April 2020 entstanden war, aber dennoch auf Februar 2020 datiert gewesen ist. Jedenfalls wurde die Forderung zehn Tage nach ihrer Einmeldung von der Klägerin beglichen.

Im Klageverfahren ging es um eine ehemalige Forderung einer großen Bank von über 20.000 Euro. Für die Hauptforderung hatte diese im Jahr 2007 einen Titel in Form eines Vollstreckungsbescheides erwirkt. Im Anschluss an die Titulierung begann der Betroffene die offene Forderung in monatlichen Raten von 50 Euro abzuzahlen. Seit 2014 wurde die Forderung nach einem Schuldenbereinigungsplan bedient, weshalb der Kläger monatliche Raten von über 200 Euro zahlte. Sechs Jahre später wurde die Forderung als erledigt vermerkt. Auch hier wurde der Löschungsaufforderung nicht nachgekommen. Vielmehr sollte sogar eine Speicherung von weiteren drei Jahren bis 2023 gerechtfertigt sein. Der Zeitstrahl über den Negativeintrag hätte 16 Jahre abgedeckt.

Zu einem Urteil kam es in keinem der beiden Fälle. Kurz vor Jahresende 2020 erklärte die Schufa, dass in beiden Verfahren eine Löschung der Einträge erfolge und sie sich dazu bereit erkläre, die Kosten des jeweiligen Verfahrens zu übernehmen. Die Vorgehensweise ist für die Schufa, die in den Verfahren Beteiligte war, typisch: Wenn sie erkennt, dass sie im Prozess unterliegen wird, kommt sie dem Klageanliegen nach, so dass das Gericht das Verfahren für erledigt erklären muss. Die Schufa vermeidet somit ein Urteil, auf das sich andere Betroffene möglicherweise berufen könnten.

Datenschutzrechtlich könnte das Verfahren aber nachwirken. Das VG nahm hier vor allem die Datenschutzbehörde in die Pflicht die Löschbegehren von betroffenen Verbrauchern ernst zu nehmen. Eine pauschale oder oberflächliche Prüfung wird dem Recht auf Vergessenwerden, dem Löschanspruch nach der DSGVO, nicht gerecht. So war es aber hier geschehen. Im ersten Fall hatte die Behörde den Löschantrag 48 Stunden lang „geprüft". Im wesentlich komplexeren, zweiten Fall hat die Behörde sich nur 24 Stunden mit dem Antrag auseinandergesetzt, bevor sie ihn ablehnte. Statt eine tatsächliche Prüfung vorzunehmen und die widerstreitenden Positionen zu bewerten, zog diese sich auf den Verhaltenskodex der Schufa (Code of Conduct) zurück und vertrat die Ansicht, dass dieses Vorgehen eine ausreichende Prüfung darstellen würde. Eine inhaltlich nachvollziehbare Argumentation war nicht gegeben.

Das Gericht brachte deutlich zum Ausdruck, dass der Verhaltenskodex der Auskunfteien nicht dazu führe, dass keinerlei Einzelfallprüfung mehr erfolgen müsse. Zudem könne das Ergebnis einer Abwägung zwischen den Grundrechten und Grundfreiheiten der betroffenen Person und den Interessen des Verantwortlichen, so wie dies von der DSGVO gefordert wird, nicht pauschal mit einer Speicherfrist von drei Jahren festgelegt werden. Vielmehr sei eine Einzelfallprüfung im jeweiligen Kontext durchzuführen.

Die DSGVO verlangt für jede Verarbeitung von personenbezogenen Daten eine Rechtsgrundlage. Daten müssen gelöscht werden, wenn der Speicherzweck erreicht wurde. Die Speicherung in einer Auskunftei setzt ein berechtigtes Interesse gemäß Art. 6 Abs. 1 lit. f DSGVO voraus. Dieses berechtigte Interesse muss begründet und dokumentiert sein. Vor allem muss es den Interessen der Betroffenen gegenübergestellt und als vorzugswürdig eingestuft werden.

Das war in diesen Fällen nicht geschehen. Besonders bedenklich ist dabei, dass hier die zuständige Aufsichtsbehörde die Vorgaben der DSGVO nicht ansatzweise beachtet zu haben scheint. Stattdessen wurde der Fall einseitig bewertet und die Verweigerung der Löschung mit einem Verhaltenskodex gerechtfertigt. Ein solches Vorgehen wird dem Umstand nicht gerecht, dass mit einem Negativeintrag der Schufa oftmals schwerwiegende Konsequenzen für die Betroffenen einhergehen.

Die Löschpflicht ist eine der wichtigsten Säulen der DSGVO. Sie umzusetzen fällt in der Praxis vielen Unternehmen nicht leicht. Ein funktionierendes Löschkonzept bleibt somit weiterhin eine der größten Herausforderungen im Datenschutzrecht. Betroffene sollten wachsam sein, sich mit einer Verweigerung der Löschung nicht immer begnügen und eine solche hinterfragen. Das gilt umso mehr, wenn die Weigerung unzureichend begründet oder gar un-

rechtmäßig erfolgt und dadurch das alltägliche Leben negativ beeinflusst wird. Der Umstand, dass sich zusätzlich eine Behörde mit dem Fall beschäftigt hat, sollte Betroffene nicht immer davon abhalten ihr Recht einzufordern. Zwar leisten die deutschen Aufsichtsbehörden oft gute Arbeit, aber unfehlbar sind sie nicht (Löschbegehren gegen SCHUFA-Eintrag – Gericht rügt HBDI, www.dr-datenschutz.de 15.01.2021).

OLG Düsseldorf

Kartellamtsverfügung gegen Facebook geht zum EuGH

Das Oberlandesgericht Düsseldorf (OLG) zeigte in seinem Beschluss vom 24.03.2021 erhebliche Zweifel am Vorgehen des Bundeskartellamtes unter der Leitung von Andreas Mundt gegen Facebook und legte dem Europäischen Gerichtshof (EuGH) in Luxemburg die Frage vor, inwieweit Wettbewerbshüter Datenschutzerwägungen berücksichtigen dürfen (Az. B6 – 22/16). Der Vorsitzende Richter des Kartellsenats, Jürgen Kühnen, erklärte nach vierstündiger Verhandlung, das Kartellamt habe sich bei seinem Vorgehen gegen Facebook zu sehr auf deutsches Recht gestützt und EU-Recht vernachlässigt.

Der EuGH soll grundsätzlich klären, ob das Bundeskartellamt der Daten-Sammelwut von Facebook aus Gründen des Datenschutzes einen Riegel vorschieben kann, und ob der US-Internetkonzern eine marktbeherrschende Stellung ausnutzt, indem er Daten seiner Nutzer und Nutzerinnen unter Verstoß gegen Regeln des Datenschutzes sammelt und verwendet. Dazu erklärte der Kartellrechts-Professor Rupprecht Podszun: „Das ist eine Delikatesse, über so etwas können wir Kartellrechtler jahrelang auf Konferenzen streiten. Wenn das Kartellamt sagt, heute machen wir Datenschutzrecht und morgen noch Arbeitsrecht – wo ist da die Grenze?" Er selbst halte Facebooks Datensammlung für einen echten Kartellfall.

Der Kernvorwurf der Wettbewerbshüter ist grundsätzlich: Anbieter wie Facebook sind so groß, dass die Nutzer auf sie angewiesen sind, so Mundt: „Den Kunden wird keine Wahl gelassen. Entweder sie akzeptieren oder sie werden abgeschaltet." Das Bundeskartellamt betrat 2019 juristisches Neuland, indem es eine „interne Entflechtung" von Facebook forderte. Die Behörde hatte dem Konzern untersagt, Nutzerdaten der Facebook-Töchter WhatsApp und Instagram sowie von Webseiten anderer Anbieter ohne ausdrückliche Zustimmung der Nutzer und Nutzerinnen mit deren Facebook-Konten zu verknüpfen. Falls die User ihre Erlaubnis nicht geben, dürfe Facebook sie nicht von den Diensten ausschließen (DANA 2/2019, 84 f.).

Der US-Konzern weist die Vorwürfe zurück. Von einer Marktbeherrschung könne angesichts der Konkurrenz durch Twitter, Snapchat oder Youtube keine Rede sein. Zudem entsprächen die Geschäftsbedingungen und die Methode der Datenverarbeitung der gängigen Praxis der Wettbewerber. Außerdem habe die Transparenz der Datenverarbeitung im Laufe der Zeit zugenommen, das gelte auch für die Möglichkeit der User bestimmte Verwertungen einzuschränken.

Gegen den Beschluss des Kartellamts wehrt sich Facebook vor Gericht. In einem Eilverfahren hatte das OLG Düsseldorf Mitte 2019 die Kartellamtsanordnungen ausgesetzt (DANA 4/2019, 239 f.). 2020 hatte der Bundesgerichtshof (BGH) jedoch wiederum die Entscheidung des OLG außer Kraft gesetzt und dem Kartellamt Recht gegeben (DANA 3/2020, 210 f.). Der Vorsitzende Richter am BGH, Peter Meier-Beck, hatte damals zur Begründung gesagt, das Gericht habe weder ernsthafte Zweifel an der marktbeherrschenden Stellung von Facebook noch daran, dass das Unternehmen diese marktbeherrschende Stellung mit den vom Kartellamt untersagten Nutzungsbedingungen „missbräuchlich ausnutzt."

Nach dem Eil- geht es nun um das Hauptsacheverfahren, in dem gründlicher geprüft wird. OLG-Senatsvorsitzender Kühnen machte dabei deutlich, dass sich sein Senat nicht an die Sichtweise des BGH gebunden fühlt. Das Kartellamt habe unter anderem eine Behinderung des Wettbewerbs durch Facebook nicht nachweisen können. Es gehe um EU-Recht, das Kartellamt habe sich fälschlich auf das deutsche Wettbewerbsrecht gestützt. Kühnen bezweifelte zudem, dass Facebook Wettbewerber mit seinen Nutzungsbedingungen behindert. Womöglich wünschten sich Nutzer ja auch in einem perfekt funktionierenden Wettbewerb, dass soziale Netzwerke ihnen maßgeschneiderte Werbung präsentieren statt irrelevanter Annoncen. Auch sei das Kartellamt keine Datenschutzbehörde. Das Verbot des Kartellamts richte sich gegen alle Facebook-Gesellschaften, diese seien aber nicht alle gehört worden.

Kartellamts-Vertreter Jörg Nothdurft meinte dagegen, das deutsche Recht sei sehr wohl das richtige und gerade für datengetriebene Geschäftsmodelle geeignet. Auch Präsident Mundt bedauerte die Entscheidung des OLG: „Eine endgültige höchstrichterliche Klärung durch den Bundesgerichtshof wird dadurch leider verzögert. Wir bedauern das natürlich im Lichte der Unterstützung, die unsere Entscheidung im Eilverfahren durch den Bundesgerichtshof erfahren hat."

Facebooks Anwälte begrüßten die OLG-Entscheidung. Die Verfügung des Kartellamts sei nun insgesamt aufzuheben. Die Behörde habe nicht bewiesen, dass sich Facebook anders verhalte als ein imaginärer Netzwerkkonzern in einem perfekt funktionierenden Wettbewerb: „Wir reden hier über ein Kartellverfahren, nicht über ein Verbraucherverfahren."

Das Bundeskartellamt legt sich immer wieder mit Internet-Riesen an. Im jüngsten Verfahren – Oculus – geht es um eine Virtual-Reality-Brille, die man nur mit einem Facebook-Account nutzen kann. Facebook macht die Nutzung der Brille davon abhängig, dass man einem Austausch der Daten zwischen Oculus und Facebook zustimmt. Hierzu Mundt: „Diese Verknüpfung zwischen Virtual-Reality-Produkten und dem sozialen Netzwerk des Konzerns könnte einen verbotenen Missbrauch einer marktbeherrschenden Stellung durch Facebook darstellen." Seine Behörde ist auch gegen den Internethändler Amazon eingeschritten. Nach einer Intervention des Kartellamts hat Amazon den über 300.000 Händlern, die über den Amazon-Marketplace verkaufen, für sie günstigere Geschäftsbedingungen eingeräumt. Sie profitieren jetzt von besseren Kündigungsfristen. Zu-

dem muss Amazon nun Gründe für eine mögliche Kündigung nennen und kann sich nicht länger von jeder Haftung gegenüber den Händlern freizeichnen. In einem weiteren Verfahren überprüfen die Wettbewerbshüter, ob Amazon Händler, die sich zu Beginn der Coronakrise mit Mondpreisen etwa für Masken bereichern wollten, zu Recht gesperrt hat oder nicht (Jahberg, Facebook-Streit landet vor dem EuGH, www.tagesspiegel.de 24.03.2021; Brühl/Hurtz/Müller-Arnold, Likes vom Oberlandesgericht, SZ 25.03.2021, 17).

OLG Hamburg

Vermögensfragen von Politikern sind keine Privatsache

Das Oberlandesgericht Hamburg (OLG) hat mit Kostenbeschluss entschieden, dass Bundesgesundheitsminister Jens Spahn ein weitreichendes Informationsinteresse der Öffentlichkeit an seinen privaten Vermögens- beziehungsweise Immobilienverhältnissen hinnehmen muss (Az.: 7 U 16/21). Spahn und sein Ehemann Daniel Funke hatten sich gegen die Berichterstattung des „Tagesspiegels“ über den Kauf einer vier Millionen Euro teuren Villa in Berlin gewendet. Das Landgericht Hamburg (LG) hatte zuvor die Ansicht vertreten, dass die Berichterstattung inklusive Erkundigungen beim Grundbuchamt zu weit gegangen sei und hatte eine einstweilige Verfügung erlassen (siehe oben S. 117). Spahn hatte sich seinerseits dafür interessiert, welche Journalisten Auskunft verlangt hatten, sich dann aber juristisch zurückgezogen.

Vor dem OLG ging es nur um eine Kostenentscheidung. Diese fiel zuungunsten Spahns und seines Ehemanns aus. Sie hätten, so das OLG, „wegen der überragenden Bekanntheit des Antragstellers“ als einem „der profiliertesten deutschen Politiker“ hinzunehmen, „dass in deutlich weiterem Umfang über ihre Vermögensverhältnisse berichtet wird, als dies für reine Privatpersonen gilt“. „Politische Führungspersonen müssen sich als Repräsentanten des Staates schon grundsätzlich eine kritische Befassung mit ihren finanziellen Verhältnissen gefallen lassen“. Für die „politische Meinungsbildung“ sei es „auch von ganz erheblichem Interesse, wie gewählte Volksvertreter ihren Lebensunterhalt bestreiten und wie sie finanziell situiert sind“.

Dies könne der Öffentlichkeit Vermutungen oder sogar „Rückschlüsse auf ihre politische Unabhängigkeit, auf ihren Geschäftssinn, aber auch auf ihre politische Ausrichtung ermöglichen. Der Erwerb einer ungewöhnlich teuren Immobilie, die für durchschnittliche Verdiener außerhalb jeder Reichweite ist und auch mit der Vergütung eines Bundesministers nicht ohne weiteres zu bezahlen ist, kann zudem Anlass zu Diskussionen über das generelle Preisgefüge am Immobilienmarkt geben.“

Da sich Spahn mit pointierten Aussagen als „besonders streitbarer Vertreter einer konservativen Politikrichtung“ profiliert und etwa geäußert habe, dass die staatliche Grundsicherung (Hartz IV) ausreichend sei, müsse er sich „eher als andere Personen eine kritische Berichterstattung über seine Vermögens- und Einkommensverhältnisse gefallen lassen“. Dies wirke sich „als unvermeidbarer Reflex“ auch auf seinen Ehemann aus. Dieser müsse die Berichterstattung dulden, da er sich immer wieder mit dem Minister in der Öffentlichkeit zeige.

Eine klare Absage erteilten die Richter auch den vorinstanzlichen Erwägungen, wonach die Informationen zur Finanzierung rechtswidrig „durchgestochen“ worden seien und deshalb nicht hätten berichtet werden dürfen. Auch in diesem Fall überwiegt nach ihrer Ansicht das Interesse der Öffentlichkeit. Das Grundbuchamt habe den Kaufpreis berechtigterweise herausgegeben: Das Grundrecht auf Pressefreiheit begründe ein schutzwürdiges Interesse der Presse am Zugang zu Datensammlungen und Registern wie dem Grundbuch, die nur in beschränktem Umfang zugänglich seien.

Im Kern ging es bei der Entscheidung nur noch darum, wer für den Rechtsstreit zahlen muss. Spahn hatte es abgelehnt, die Kosten zu tragen, muss aber nun gemäß dem OLG-Beschluss drei Viertel, geschätzte 10.000 €, zahlen (Die teure Villa in Berlin, www.faz.net 27.04.2021; Heidtmann, Nicht wirklich privat, SZ 29.04.2021, 25; Müller-Neuhof, Gericht stuft Spahns Villenkauf als politisches Thema ein, www.tagesspiegel.de 28.04.2021).

LG München I

BMG-Kooperation mit Google kartellrechtswidrig

Gemäß zweier Beschlüsse der 37. Zivilkammer des Münchener Landgerichts I (LG) in einstweiligen Verfügungsverfahren ist die Kooperation zwischen dem Bundesgesundheitsministerium und Google kartellrechtswidrig (Az. 37 O 15720 u. 15721/20). Das Gericht hat damit den Anträgen von NetDoktor.de, das zum Burda-Verlag gehört, stattgegeben und festgestellt, dass die Vereinbarung Informationen eines Portals des Bundesgesundheitsministeriums (BMG) in den Knowledge Panels von Google anzuzeigen unzulässig ist. Die zuständige Zivilkammer hat entsprechend die Zusammenarbeit des Ministeriums und des Suchmaschinenanbieters vorläufig untersagt. NetDoktor.de führte unter anderem an, dass seit der Bevorzugung von Google seine eigenen Klickzahlen teilweise bis zu 30% zurückgegangen seien, obwohl das Google-Ranking mehr oder weniger gleichgeblieben war. Das wiederum führe zu Abwanderungstendenzen bei Werbekunden bei NetDoktor.de.

In der Begründung der Vorsitzenden Richterin Dr. Gesa Lutz heißt es: „Das BMG ist mit Google eine Vereinbarung eingegangen, die eine Beschränkung des Wettbewerbs auf dem Markt für Gesundheitsportale bewirkt“. Die bestmögliche Position in den Suchergebnissen, also die Infobox, stünde privaten Anbietern von Gesundheitsportalen nicht mehr zur Verfügung. NetDoktor.de sei angewiesen auf die Sichtbarkeit bei Google, die durch die Infoboxen stark eingeschränkt wird, was wiederum zu einem verringerten Nutzeraufkommen bei NetDoktor.de führt und damit potenziell zu einem Verlust von Werbeeinnahmen.

Anders als das Gesundheitsministerium bisher argumentierte, stellte Lutz fest: „Die Zusammenarbeit von Google und dem BMG ist auch nicht wegen qualitativer Effizienzgewinne, etwa wegen einer Verringerung des Suchaufwands für die Nutzer oder einer Verbesserung

der Gesundheitsaufklärung der Bevölkerung durch die Infoboxen, ausnahmsweise zulässig." Die Nachteile würden so nicht aufgewogen, wozu auch eine Reduzierung der Medien- und Meinungsfreiheit gehöre.

Die Beschlüsse sind noch nicht rechtskräftig. Die Kammer hat zudem nicht entschieden, ob das Ministerium überhaupt ein solches Informationsportal betreiben darf. Ein Antrag auf einseitig marktmissbräuchliches Verhalten von Google wurde aus formellen Gründen zurückgewiesen.

Bundesgesundheitsminister Jens Spahn und der für Europa zuständige Google-Vizepräsident Philipp Justus hatten die Kooperation im November 2020 bekannt gegeben. 160 Gesundheitsthemen sollten seither bei der Suche prominent als Knowledge Panel angezeigt werden – die Informationen stammen allesamt vom Portal gesund.bund.de. Neben NetDoktor.de klagt auch der „Wort & Bild"-Verlag, dem die Apothekenumschau angehört. Die Medienanstalt Schleswig-Holstein/Hamburg hat ebenfalls ein Verfahren eingeleitet, da das Portal den Medienstaatsvertrag verletzen könnte.

Nach der Entscheidungsverkündung zeigte sich der Burda-Justiziar Maximilian Preisser erfreut und pries die Beschlüsse als Sieg „für die gesamte Presse". Das BMG teilte mit, man werde „das Urteil zur Kenntnis nehmen" und nach dessen Auswertung über weitere Schritte entscheiden. Google erklärte: „Wir sind enttäuscht darüber, dass das Landgericht München die Einbindung von faktischen und wissenschaftlichen Informationen in die Google Suche nun untersagt hat. Wir prüfen die Entscheidung und die uns zur Verfügung stehenden Rechtsmittel" („Netdoktor gegen BRD und Google: Vereinbarung über Knowledge Panels kartellrechtswidrig", www.justiz.bayern.de 10.02.2021; Weiß, Gericht untersagt Kooperation von Gesundheitsministerium mit Google, www.heise.de 10.02.2021, Kurzlink: https://heise.de/-5051197; Handel, Urteil nach Burda-Klage, SZ 11.02.2021, 23).

Buchbesprechungen



Thüsing, Gregor
Beschäftigtendatenschutz und Compliance
C.H.Beck-Verlag München,
3. Aufl. 2021
ISBN 978 3 406 71502 0, 393 S.,
129,00 €

(tw) Es gibt nicht nur viele Darstellungen und Abhandlungen zum Datenschutz allgemein, sondern auch zum Beschäftigtendatenschutz speziell. Stärker noch als bei den allgemeinen Darstellungen ist beim Literaturstudium über die arbeitsrechtliche Digitalisierung zu hinterfragen, wessen Lied hier jeweils gesungen wird – das der Arbeitgeber oder der Arbeitnehmer? Insofern wird bei dem Handbuch von Thüsing schnell klar: Adressiert wird der Unternehmensjurist, nicht die oder der Beschäftigte. Letztgenannte interessieren sich rollenbedingt nicht für „Compliance". Sie dürften schon im Vorwort schlucken, wenn dort beim Datenschutz vor dem „Eifer des Zeloten" – also des Einäugigen – gewarnt wird. Nicht nur dieses Bild, auch der einleitende elaborierte Sprachgebrauch adressiert offenbar eher den Akademiker in der Unternehmensleitung als den Betriebsrat.

Steigt der Rezensent dann in die Tiefen des Werks ein, so muss er regelmäßig sein zunächst gefasstes Vorurteil revidieren: Diese systematische Darstellung des Beschäftigtendatenschutzes ist weitgehend ausgewogen, mit guten und vielen Quellen belegt und geht an vielen Punkten tiefer, als das von anderen Darstellungen gekannt wird; so spricht sie z.B. immer wieder mal auch internationale Bezüge an. Dies hindert den Autor bzw. die Autoren aber nicht, eine eher unternehmensorientierte Argumentation zu verfolgen, etwa wenn es um die Anwendung des Telekommunikations(TK-)geheimnisses und des TK-Gesetzes bei der Erlaubnis privater Nutzung von TK-Anlagen geht, was entgegen der herrschenden Meinung – aber mit erwägenswerten Gründen – abgelehnt wird.

Zwar steht auf dem Umschlag des Werks „Thüsing", doch sind neben dem Bonner Arbeitsrechtler vier weitere Autoren drin, die alle dem „Stall" von Thüsing zugeordnet werden können: Gerrit Forst, Stephan Pötters, Thomas Granetzky und Johannes Traut. Diese, wohl hauptverantwortlich für die jeweils gemeinsam mit Thüsing gezeichneten Texte, haben sich auch schon anderweitig wissenschaftliche Sporen verdient.

Anders als andere renommierte Handbücher zum Beschäftigtendatenschutz, etwa den „Gläsernen Belegschaften" von Wolfgang Däubler, fällt bei der Lektüre auf, dass das Werk Schwergewichte legt und dabei zugleich wichtige Inhalte vernachlässigt: So wird der Beschäftigtendatenschutz in das übergeordnete Thema Compliance eingeordnet, was dazu führt, dass z.B. dem Whistleblowing ein wichtiger Platz zugewiesen wird. Complianceaufgaben der Unternehmensleitung werden umfassend abgeleitet und begründet. Das Betriebsverfassungsrecht und insbesondere die §§ 87 Abs. 1 Nr. 6 und 80 Abs. 2

werden ausführlich behandelt, aber die Funktion der Mitbestimmung beim Datenschutz nur kursorisch. Unter der Überschrift „personengebundene Merkmale" wird der Biometrieeinsatz ausführlich erörtert; die praktisch erheblich bedeutendere Verarbeitung von Gesundheitsdaten wird dagegen in einem knappen „Exkurs" behandelt. Weitere Schwerpunkte sind Datenabgleiche, E-Mail-Nutzung, Videoüberwachung, Mobilitätsüberwachung, Social Media oder Haftung. Automatisierte Entscheidungen finden keine Erwähnung; Betroffenenrechte werden unter der Überschrift „Absicherung des materiellen Datenschutzes durch Transparenz, Organisationspflichten und Dokumentation" sehr selektiv abgehandelt. Und beim internationalen Datenverkehr wird die zentrale Entscheidung des EuGH zu „Schrems II" zwar erwähnt, die damit verbundenen Konsequenzen aber nur oberflächlich behandelt. Ein Grund für die begrenzte Aktualität des 2021 veröffentlichten Buchs lässt sich vermuten, wenn das Vorwort vom November 2019 datiert: Möglicherweise wurde das Ursprungsmanuskript schon früher fertiggestellt und dann nur noch aktualisiert. Das Jahr 2020 war auch für juristische Buchveröffentlichungen wegen Corona ein schwieriges Jahr.

Das tut dem Wert des Buchs aber keinen Abbruch: Es ist gerade auch für arbeitnehmernahe Datenschützer und Bürgerrechtler wichtig, den Blick über den eigenen Tellerrand zu richten. Hierzu bietet der „Thüsing" Material für gediegene Recherche bei den behandelten Themen. Auch einige Checklisten oder Formulierungsvorschläge sind es wert, in der praktischen Arbeit hinzugezogen zu werden. Allein auf dieses Werk zur Beantwortung von Rechtsfragen kann man sich aber in vielen Bereichen des Beschäftigtendatenschutzes nicht verlassen.



Kipker, Dennis-Kenji/
Voskamp, Friederike (Hrsg.)
Sozialdatenschutz in der Praxis
Nomos Verlag Baden Baden 2021,
582 S., ISBN 978-3-8487-5843-2,
79,00 €

(tw) Nachdem die Literaturschwemme zur DSGVO auf ein normales Maß zurückgegangen ist und allenfalls Neuauflagen das Marktgeschehen beim allgemeinen Datenschutz beleben, öffnen sich die bereichsspezifischen Datenschutzfragen der literarischen Bearbeitung. Zunächst fanden sich diese Arbeiten mit spezifischen Fragestellungen in Fachzeitschriften verteilt. Inzwischen werden die dabei erlangten Erkenntnisse in Buchform zusammengeführt. Für jemanden, der den gewaltigen Zeitschriftenmarkt kaum abdecken kann, besteht so die Möglichkeit gezielt und mit einem Griff in den Bücherschrank sich die nötigen Informationen zu besorgen.

Diese Möglichkeit besteht inzwischen auch für den Bereich des Sozialdatenschutzes, zu dem der Nomos-Verlag nach einer einschlägigen, von Krahmer herausgegebenen Gesetzeskommentierung (DANA 2/2020, 131 f.) nun das Praktikerhandbuch, herausgegeben von Kipker/Voskamp, präsentiert. Und tatsächlich ist damit gleich in der ersten Auflage eine Zusammenstellung gelungen, die viele Bedürfnisse der „Praxis" befriedigt ohne dabei auf die wissenschaftliche Tiefe zu verzichten.

Es ist eigentlich ein Ding der Unmöglichkeit das derzeit geltende Sozialdatenschutzrecht in einem Werk konsistent darzustellen und dabei zugleich den Blick für die Praxis zu wahren. Die vielen SGB-Bücher sind wort- und facettenreich. Der Datenschutz dort ist vielstufig und unübersichtlich geregelt. Doch ist das Anliegen einer umfassenden verständlichen Darstellung mit diesem Sammelwerk weitgehend gelungen, in dem Praktikerinnen und Praktiker qualifiziert ihre Bereiche darstellen. Dabei verwundert die eher untypische Gliederung, bei der nach einer allgemeinen Einführung zunächst die Betroffenenrechte und Kontrollen, dann die Verantwortlichkeiten und die technischen Entwicklungen und erst danach das allgemeine Sozialverwaltungsverfahren des SGB X dargestellt werden. Diese Reihenfolge erschließt sich aber schnell bei der Lektüre. Dem folgen vier große spezifische Kapitel zum gerichtlichen Verfahren, zur Forschung, zur Grundsicherung für Arbeitssuchende und zur Kinder- und Jugendhilfe. Zu knapp fällt dagegen das letzte Kapitel zu den Sozialversicherungen (Kranken-, Renten- und Unfallversicherung) mit nur knapp 50 Seiten aus. Doch wird auch insofern ein Überblick über die jeweils großen Felder gegeben. Die Detailrecherche macht hier aber die Zuziehung eines Spezialkommentars nötig.

Dies gilt nicht für die Bereiche Arbeitslosengrundsicherung und Kinder- und Jugendhilfe, wo auf die in der Praxis auftretenden Fragen qualifizierte Antworten gegeben werden. Beeindruckend sind die Kapitel zum Gerichtsverfahren und zur Forschung. Hier bereitet – soweit erkennbar erstmals – ein Sozialrichter (Leopold) systematisch alle relevanten Fragen auf, die vor dem Sozialgericht anfallen, wobei er viele Antworten gibt, die auf die gesamte Gerichtsbarkeit übertragbar sind. Noch ausführlicher und ins Detail gehend ist Schäfer, die nicht nur den rechtlichen Rahmen der Forschung darstellt, sondern auch viele Details aus der Praxis – und dies auf aktuellem Stand. So widmet sie sich ausführlich den Transparenzregeln nach den §§ 303a ff. SGB V mit dem Forschungsdatenzentrum, aber auch vielen weiteren Datenquellen und Forschungsstrukturen. Dass dabei die nationalen Regelungen nicht an den forschungsfreundlichen Ansprüchen der DSGVO gemessen werden, ist für ein Praktikerhandbuch verständlich, aber letztlich schade und insofern entwicklungsfähig.

Jedes der Kapitel ist eine in sich geschlossene Darstellung wodurch Redundanzen, also Mehrfachbehandlungen einzelner Themen, nicht zu vermeiden sind. Dies eröffnet aber auch den Blick auf verschiedene Sichtweisen. Durch die Praxisnähe der Autorinnen und Autoren wird oft eine pragmatische Sicht vermittelt ohne aber dabei das Grundanliegen des Persönlichkeitsschutzes, der mit der Vertraulichkeit für die soziale Arbeit wesentlich ist, in Frage zu stellen. Die Literaturauswahl ist manchmal selektiv, aber äußerst hilfreich, ebenso wie die einleitende Gliederung sowie die für ein Handbuch zentralen Verzeichnisse zu Stichworten, Literatur und Abkürzungen.

Durch die Problemorientierung der Darstellung ist dieses Buch sowohl Praktikern wie auch Wissenschaftlern sehr zu empfehlen. Angesichts des Umstands, dass gerade in Coronazeiten Bibliotheken nicht oder schwer zugänglich sind, erhält man mit diesem Handbuch eine nützliche Hilfe bei der Anwendung des Sozialdatenschutzes in die Hand.



Manfred Wernert
Internetkriminalität
Stuttgart 2021, Boorberg Verlag
ISBN: 978-3415068919

(me) Das Thema „Internetkriminalität" ist von hoher Brisanz und großer Aktualität: Das zeigt die Berichterstattung über die mit NSU 2.0 gekennzeichneten Drohschreiben, gerichtet an Personen des öffentlichen Lebens. Der mutmaßliche Täter konnte nach jahrelangen Ermittlungen gefasst werden. Er nutzte die Strukturen des Darknet. Besondere Aktualität bekommt das Thema auch durch die Zerschlagung pädophiler Netzwerke, die vor allem im Internet (im Darknet) aktiv waren. Ihre Zerschlagung gelang vor kurzem (Nachrichtenmagazin „Panorama" vom 4.5.2021).

Das Lehrbuch erscheint mittlerweile seit über zehn Jahren und ist in 4. Auflage erhältlich. Seine vorrangige Zielgruppe sind Polizeibeamte. Darüber hinaus wird nicht nur der in Informatik und Rechtswissenschaft Vorgebildete Honig aus der Lektüre saugen können, sondern auch der interessierte Laie. Verfasst wurde es von einem Dozenten der Hochschule für Polizei Baden-Württemberg, Manfred Wernert.

In der gebotenen Kürze besticht die Darstellung auf 232 Seiten durch Übersichtlichkeit und Verständlichkeit der Ausführungen. Besonders gut gelungen sind die Ausführungen zu den Rechtsgrundlagen polizeilicher Ermittlungstätigkeit und die Beschreibung der technischen Grundlagen des Cybercrime und der Gerätschaften, derer er sich bedient. Zu Recht weist der Autor darauf hin, dass das Internet als Tatort auch künftig nur begrenzt kontrollierbar sein wird. Wernert versucht die vorhandenen Kontrollmöglichkeiten wirksamer werden zu lassen und die Ermittlungsmöglichkeiten der Polizei zu beleuchten. Besondere Erscheinungsformen der Kriminalität werden im Einzelnen vorgestellt, neben den bereits benannten Feldern beispielsweise Betrug, Urheberrechtsverletzungen, Diebstahl digitaler Identitäten, „Happy Slapping[1]", u.a.

Gefallen hat nicht zuletzt die Gestaltung des Lehrbuches mit Hilfe fotografischer Darstellungen der betroffenen Hardware, erläuternden Diagrammen, einem Überblick über einschlägige Rechtsvorschriften und einem Glossar mit den wichtigsten Fachbegriffen.

1 Körperlicher Angriff auf Unbeteiligte, der gefilmt wird und dadurch die Erniedrigung der Opfer beabsichtigt.

Cartoon



Die Inspiration zu diesem Cartoon kam von einem Text auf der Internetseite einer Partei in NRW.


„Ich habe nichts zu verbergen!“
Ich bin Pfarrer, aber ich glaube nicht an Gott
Die PIN-Nummer meiner EC-Karte ist 5151
Mein Geburtsdatum? 12.09.1988 Geburtsort: Bonn
Der Zahlencode von meinem Fahrrad-schloss: 2468
Meinen 5400 Followern bei Face-book werde ich jetzt meine Adresse be-kannt geben
Das Pass-wort von meiner E-Mail-Adresse: F8jd4xxG3
Der Ersatz-schlüssel zu meiner Wohnung ist unter der Fußmatte auf der Terrasse
!
Schaut mal wie-viel Geld sich auf meinem Konto ange-sammelt hat
Und wirklich nichts zu befürchten?
Bild: iStock.com/bernardbodo